

**KENORA DISTRICT SERVICES BOARD  
POLICY and PROCEDURE**

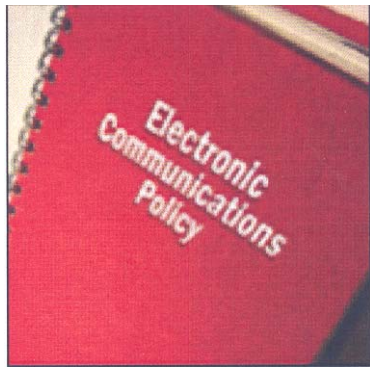
<b>TITLE: ELECTRONIC COMMUNICATIONS</b>		<b>SECTION: HUMAN RESOURCES</b>	
<b>DATE: September 10, 2001</b>		<b>POLICY NO.: KDSB-HR-I-05</b>	
<b>APPROVED BY: Resolution #2003-36</b>		<b>REVISED: Resolution #2008-74 (May 8, 2008)</b>	

**1. POLICY STATEMENT**

It is the policy of the Kenora District Services Board to encourage the use of electronic communications by Board employees as a tool to enhance their ability to perform their jobs and to keep informed on matters directly related to their jobs/duties.

Effective use of electronic communications relies upon end users adhering to principles of appropriate standards of proper conduct. In general, this requires the efficient, ethical and legal utilization of network resources by Board employees.

The attached policy defines the responsibilities of the Kenora District Services Board employees using KDSB electronic communication resources.



**ELECTRONIC COMMUNICATIONS**

**POLICY**

**Kenora District Services Board**

April 10, 2008

## **General**

### **Electronic Communications Policy**

This Electronic Communications Policy ("Policy") outlines the policies and guidelines that must be followed at all times to minimize business risks and maximize the benefits of electronic communications within the Kenora District Services Board (also referred to in this Policy as "KDSB"). This Electronic Communications Policy has been adopted by the Board of Directors of KDSB as of May 8, 2008. All employees of KDSB must comply with the terms of this Policy immediately. Managers, employees and technical personnel must modify system configurations and procedures, if necessary, to comply with the terms of this Policy as promptly as possible, with the goal of doing so within ninety (90) business days following adoption or amendment.

### **Relation to Laws and Other Policies**

This Policy should be reviewed in conjunction with other KDSB policies generally. The management of electronic communications records in electronic form and as printed out is subject to federal and provincial laws as well as KDSB records management policies, including their provisions regarding retention and disclosure. In some circumstances, the laws of other countries may be applicable.

### **Electronic Communications Resources**

KDSB owns, has a property interest in or has a right to specify the use of:

- all information (owned or personal information about the users or content that is personal to the users), information processing and communications facilities employed in its business, including computers, fax machines, telephones, smart phones, pagers, wireless email devices, copiers, software, on line accounts, email facilities, facilities for Internet/ Intranet/Extranet access, storage media, network accounts, computer and email and instant messaging files and messages and related equipment and documentation employed or stored in its offices and the facilities at KDSB's disaster recovery site; and
- all such information, information processing and communications facilities employed in its business that are connected to or able to be connected to its facilities from locations outside of KDSB's premises, including personal information processing and communications equipment and software owned or leased by KDSB personnel or supplied by KDSB to KDSB personnel for their use, as necessary, in connection with KDSB's disaster recovery plan.

All such resources are collectively referred to in this Policy as "Electronic Communications Resources" or "Resources." References to the "KDSB network" include the Electronic Communications Resources at and connected to KDSB's disaster recovery site.

NOTE: Only Electronic Communication Resources owned, leased or that KDSB has a proprietary interest in may be:

- (1) used to conduct KDSB business;
- (2) connected to KDSB information processing and communications facilities, without the prior written approval of KDSB.

## **Purposes**

The purposes of this Electronic Communications Policy are to:

- establish policies on privacy, confidentiality, and security in electronic communications;
- ensure that Electronic Communications Resources are used for purposes appropriate to KDSB's business;
- inform all employees of KDSB about the applicability of laws and policies to electronic communications;
- ensure that Electronic Communications Resources are used in compliance with those laws and policies;
- provide guidance concerning rights and responsibilities with respect to the proper use of Electronic Communications Resources; and
- protect information pursuant to the Personal Health Information Protection Act (PHIPA); the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and Personal Information Protection and Electronic Documents Act (PIPEDA).

## **Scope**

This Policy applies to:

- all Electronic Communications Resources owned, leased or managed by KDSB;
- all Users and uses of KDSB Electronic Communications Resources;
- all KDSB electronic communications records in the possession of KDSB Authorized Users; and
- the contents of electronic communications, and to the electronic attachments and transactional information, including personal information associated with such communications.

## **Indirect Violations**

KDSB expects that all Users will honour the spirit and intent of this Policy and the goals that this Policy is intended to achieve. They should not attempt to do indirectly what this Policy prohibits directly, and they should not employ means to defeat the goals that this Policy is intended to achieve, even though those means may not have been mentioned in this Policy.

While KDSB has endeavored to have this Policy reflect the state of KDSB's technology as of the date of its adoption, technological developments may outstrip the literal text of certain aspects of this Policy. If you are in doubt, ask questions and seek advice before acting.

## **Authority**

KDSB reserves the right to amend, revise or withdraw this Policy and to add any rules, policies, or procedures to this Policy at any time. KDSB personnel will be notified of any such amendment.

In all situations, KDSB personnel are expected to use the Electronic Communications Resources in a manner that can be supported by KDSB, and to exercise good judgment in the discharge of their responsibilities with respect to the Resources.

Changes to this Policy require approval by the Board of Directors of KDSB. Changes in operating procedures, standards, guidelines and technologies, may be authorized by the Chief Administrative Officer (CAO).

The primary responsibility for enforcement of this Policy and its operating procedures rests with the CAO and KDSB employees. Senior management is responsible for ensuring the directives are implemented and administered in compliance with the approved Policy.

## Definitions

### Alias

An alternative name or electronic identification for oneself. An alias can be anything from a corporate name, a business department or a personal nickname (e.g. [sales@domain.com](mailto:sales@domain.com), [abuse@domain.com](mailto:abuse@domain.com), [firstnameonly@domain.com](mailto:firstnameonly@domain.com)). Mail sent to an email alias will be directed to the email address for that alias.

### Attachment

An attachment includes any file that is included with or attached to an electronic communication between an originator and a receiver.

### Authorized User

Authorized User means any person who uses the Electronic Communication Resources with proper authority. The term includes employees of KDSB who have completed the required prerequisites for use and persons who are not employees and have been properly authorized to use the Electronic Communication Resources.

### Blind Carbon Copy (Bcc)

This term means that an original or carbon copied recipient will not know that a copy of the message is going to another person.

### Carbon Copy (Cc)

Like in a written letter, the carbon copy "Cc:" is a message that is addressed to another person in addition to the addressee(s), that is, the person or persons in the "To:" line.

### Chain Letter

Email intended to be sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

### Denial of Service (DOS) Attack

A method of attacking a server by sending an abnormally high volume of requests over a network, which essentially slows down the performance of a server, such that the server is unavailable for Authorized Users.

### Electronic Communications

Any communication transmitted electronically via the use of the Electronic Communications Resources.

### Electronic Communications Resources

See definition in section above.

### Electronic Mail

The term "Electronic Mail" or "Email" is any information that is transmitted electronically through a mail protocol such as SMTP or IMAP.

## Email-bomb

An email-bomb is characterized by abusers repeatedly sending an email message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact.

## Email Signature

An email signature is information that is included at the end of your email messages to give the recipient more information about you. It usually contains your name, title, address, phone number, etc.

## Forward

The action of sending an email message received to someone other than the intended original recipient(s).

## Instant Messaging

A service that alerts users when friends or colleagues are online and allows them to communicate with each other in real time through private online chat areas.

## Mailbox

An electronic mailbox receives and stores email messages until they can be retrieved by a recipient.

## Malicious Code

Malicious code takes many forms, including viruses, worms, Trojan Horses, and spy ware. Malicious code can be transmitted in attachments to an email, by downloading infected programming from other sites, and can be present on a diskette or CD. Creators of malicious code are extremely inventive and constant vigilance is required to avoid infection.

## Newsgroup

An online discussion group. Newsgroups are sometimes called Forums.

## Phishing

A phish is an email message that is designed to appear as though it came from a financial institution, government agency or commercial site and is intended to deceive the user into revealing sensitive information such as bank account numbers, passwords, and social security or other national identification numbers. The sensitive information can be personal or corporate. Thereafter the phisher typically uses the information for purposes of theft or sells the information to others who may use the information for purposes of theft.

## Spam

Spam (also called "Unsolicited Commercial Email" or "UCE") is a term used to describe an email with many copies that is sent out over the Internet in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or ghazi-legal services. This type of message can also contain Malicious Code.

## Subject Line

The location in the email where you put the topic of your message.

## Web-Based Email

An email account that is accessed through a Web browser, such as Microsoft Internet Explorer.

### White Hat

A type of hacker who identifies security vulnerability in a computer system or network primarily to expose the vulnerability to the administrators so that it can be fixed before it can be taken advantage of by others.

## Usage Rules

### Ownership

KDSB owns, leases or has the right to specify the use of all Electronic Communications Resources. No employee has any property interest in the Electronic Communications Resources.

### Authorized Users

Employees of KDSB are eligible to use the Electronic Communications Resources but may do so only in accordance with this Policy.

The prerequisites to KDSB employees obtaining access to KDSB's Electronic Communications Resources include the following:

- a) An approved request for access to the Resources signed by the employee's immediate supervisor; and
- b) Completion of mandatory training in the use of the Resources by the employee.

Each employee, including new hires, shall receive training on the use of KDSB's Electronic Communications Resources, with specific procedural training regarding security and controls. Emphasis on an employee's responsibilities and rights in the use of Electronic Communications Resources will be underscored.

Temporary employees and outside contractors may be given access to Electronic Communications Resources. Any outside personnel given access to KDSB's email resources are Authorized Users and are subject to the same policies as employees and must undergo the same training as specified above.

### Personal Use

#### Incidental Personal Use

KDSB's Electronic Communications Resources are a corporate asset which must be used primarily for legitimate business purposes. Personal use is strictly prohibited unless authorized in the KDSB's Electronic Communications Policy – Best Practices Guide

### Unacceptable Usage

The following activities are unacceptable and are prohibited with respect to the Resources. The list below is not exhaustive, but attempts to provide a framework for activities that fall into the category of unacceptable and prohibited use.

#### Unlawful Activities

Users must not engage in illegal or wrongful conduct.

#### Personal Gain

Electronic Communications Resources may not be used for personal gain (except as permitted under applicable personnel policies).

**Fraudulent Offers**

Users must not make fraudulent offers of products, items or services.

**Intellectual Property Infringement**

Users must not infringe the copyright or other intellectual property rights.

**Unsubstantiated Claims**

Users may not use the Electronic Communications Resources to exchange gossip or personal information about themselves or others, or rumors, exaggerated claims and unsubstantiated opinions relating to the company.

**Discrimination**

Users must not send discriminatory messages based on race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, age, record of offences, marital status, family status, disability, gender, sexual orientation, or religious or political beliefs or other basis that is protected under applicable law.

**Insensitive Language**

Users must not use offensive, derogatory or abusive language.

**Harassment**

Users shall not engage in any harassment including, but not limited to, conduct contrary to any other policy or law, use of an alias, sending or forwarding jokes or chain letters.

**Profanity**

Users must not use profanity in their electronic communications.

**Objectionable Material**

Users are prohibited from sending objectionable material such as pornography and sexually explicit jokes, letters, email messages, cards to anyone.

**Resource Restrictions**

Users shall not use the Electronic Communications Resources for purposes that could reasonably be expected to directly or indirectly cause strain on any Electronic Communications Resources, or unwarranted or unsolicited interference with others' use of the Electronic Communications Resources. The list below is not intended to be exhaustive.

**Chain Letters and Malicious Code**

Do not send or forward electronic mail chain letters or email with attachments known or suspected to contain Malicious Code.

**SPAM**

Do not send "spam."

**Email-bombs**

Do not send email bombs.

**Illegal Software**

Do not download and/or install any software without prior approval of the LSSC.

**DOS Attacks**

Do not engage in DOS Attacks.

**Automatic Forwarding**

Do not set up rules to automatically forward email received to a company email inbox to an external email address.

**Source Code**

Do not send computer source code via an email.

**External Email Systems and Personal Accounts**

**Use on Company Business**

Company-related correspondence or any company-related information must not be communicated or conducted via external email systems or personal email accounts.

**Access to External Systems Prohibited**

Accessing external email systems or personal email accounts from company-provided equipment is prohibited. This includes, but is not limited to, Yahoo! Mail, Hotmail, MSN Mail, AOL, EarthLink, and other web-based email and email services offered by Internet service providers.

**Non-Competition**

No competitive, trade secret or business information shall be transmitted unless specifically authorized.

There may be exceptions to this policy if KDSB is collaborating on a legislative matter affecting the industry, in standard setting processes and similar circumstances. If in doubt, consult your supervisor.

**False Identity and Anonymity**

Users shall not, either directly or by implication, employ a false identity (the name or electronic identification of another) or forge/attempt to forge any portion of email or instant messages. Authorized Users may use an alias (an alternative name or electronic identification for oneself), so long as the pseudonym clearly does not constitute a false identity. Authorized Users may not send email anonymously (the sender's name or electronic identification are hidden).

**Account Ownership**

Users are responsible for their own accounts. Users are prohibited from providing their account and password information to another individual. All accounts and contents are the property of KDSB.

**Email Signature**

It is required that Authorized Users use email signatures to provide relevant contact information to the recipient. Email signatures should contain your full name, job title, company name, telephone and fax numbers, and the company web address.

**Disclaimers**

Authorized Users must use disclaimers in emails and faxes sent to third parties that make clear any limitations on the extent to which the messages from the employee may be understood to have been sent on behalf of the company.

**Use of Instant Messaging (IM)**

IM allowed using company-sanctioned software  
Instant messaging may be used in connection with company business only if enterprise IM software approved by the company is used.

## Confidentiality and Security

### Email Security

Authorized Users should be aware that email messages are not secure and can be potentially accessed by others. There is no guarantee of delivery and they may be tampered with by a third party. They may also be intercepted, incorrectly addressed or easily forwarded to third parties. Therefore, employees of KDSB are to use the following guidelines regarding email use:

- Authorized Users should verify that they have selected the intended destination or recipient (i.e., JSMITH, JSMITH1, JSMITH2, etc.) prior to transmitting an email message.
- Authorized Users should not share personal mail boxes and passwords. Do not tell others your power-on or KDSB network password. Do not write these passwords down or keep notes of them except as may be required by the KDSB.
- Do not leave your email accessible when away from your desk so others can read or send a message from your PC purporting to be you, or amend or delete emails in your email account. Log off/lock your computer if you will be away from your desk.
- You will be held responsible for all inappropriate email activity from your account.
- Printed email messages should be retrieved as soon as possible to prevent unauthorized individuals from reading messages containing privileged information.
- Authorized Users must take necessary precautions when receiving emails via the Internet or even internal messages with attachments. These could contain Malicious Code and should be checked before opening.
- Never open email attachments from an unknown or unsolicited source – simply delete them.
- Do not respond to any email that asks for personal or corporate account information, passwords or similar information as it is likely to be a phish. Immediately delete it.

### Protection Against Malicious Code

- KDSB protects the network with software that scans for Malicious Code and runs both on network servers and on individual computers. For this software to be fully effective against known Malicious Code, a current set of definitions of such code must be stored on every computer connected to the network. These definitions are updated as soon as the software vendor makes an update available and are automatically updated on each network computer when it boots up. All Authorized users must reboot their computers every day.
- Authorized Users are responsible for seeing to it that their computers and/or laptops are running the current definitions of Malicious Code. Hence, Authorized users who have been issued laptops must bring their laptops into the LSSC at least monthly so that the most recent definitions may be installed.
- Authorized Users must have software that scans for malicious code and is approved by the LSSC on their home computers if they transport files from their home machines to the network. They must ensure that this software is kept current.
- If an Authorized User suspects that the Resources he or she uses have been infected by Malicious Code, do not attempt to eradicate the code without expert assistance. Rather, do the following immediately:

- a) disconnect from all networks,
  - b) call the LSSC; and
  - c) shut down the computers involved.
- Authorized Users are prohibited from disabling anti-virus software running on company-provided computer equipment as provided and maintained by the LSSC.

### **Passwords**

- Security password features have been put in place to reduce potential unauthorized access to the KDSB network. Network login passwords must be changed every ninety (90) days, network login passwords cannot be reused and three (3) incorrect network login attempts will result in Authorized User accounts being made inoperable.
- If an Authorized User suspects that a password has been disclosed to unauthorized parties, he or she must notify the LSSC immediately and passwords must be promptly changed.
- All passwords created by Authorized Users must be at least eight characters long, must contain at least one upper and one lower case alphabetic character and at least one non-alphabetic character. Non-alphabetic characters include numbers (0-9) and punctuation (example: Wed6%0L).
- In order to be effective, passwords created by Authorized Users must be difficult to guess. Derivative of User-IDs must not be used. Personal data like spouse's name, birthday, child's name, and pet's name are easy to compromise, unless accompanied by additional characters. Passwords with common keyboard sequences such as "ZXCVBNM" or "!@#&%^" or words found in a dictionary must not be used. Slang, common company or business acronyms and geographical names must not be used unless accompanied by additional characters.
- Do not construct fixed passwords by combining a set of characters that do not change with a set of characters that change predictably. Predictable passwords that change are typically based on the month, a department, a project, or some other easily-guessed factor. For example, do not employ passwords like "AZ9JAN" in January, "AZ9FEB" in February, etc.
- Do not use passwords that are substantially similar to previously used passwords.
- Do not store passwords in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, computers without access control or in other locations where unauthorized persons might discover or use them.
- Do not send passwords (for corporate subscriptions, e-commerce sites, vendor intranets, online portals, etc.) or other critical data like credit card information via email or other unsecured electronic methods.
- Do not write passwords down and leave them in a place where unauthorized persons might discover them unless (1) such passwords are effectively concealed in a phone number or in other seemingly unrelated characters or (2) a coding system has been used to conceal the password.
- Do not use dial-up communications programs or Internet browsers to store fixed passwords at any time.
- Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the Authorized User.

## Email Encryption

### **Only specified forms of encryption are permitted**

When required by KDSB, Employees will encrypt their electronic communications and files with the use of software approved by the KDSB. This software will provide for retention by the company of any key necessary to access encrypted messages. Keys must be kept under the secure control of the LSSC at all times. Readable versions of private keys may not be stored on personal computer hard disks. Encryption methods not approved by the LSSC, including use of proprietary encryption algorithms, are prohibited for any purpose as it would hinder proper investigations or audits.

## Confidentiality

During the course of performing company-related duties, employees of KDSB may hear or acquire a great deal of confidential information about the company, present and prospective clients, suppliers, and other KDSB employees or Board members. Examples of confidential information include but are not limited to: corporate strategies (not yet released to the public), personal employee data or information, trade secrets, property sales/acquisition or security, solicitor advice or opinions, personal information of clients, and research data.

### **Obligation of Confidentiality**

Confidential information must be held in the strictest of confidence during the term of employment and after termination for any reason. It is to be used solely for KDSB purposes and never for personal gain. Under no circumstances should such information be transmitted to persons outside KDSB, including family or associates, or to other KDSB personnel (unless they have a specific need to know information to discharge their duties). The only exceptions to this policy would be routine credit or income inquiries, information released in the normal course of business, disclosures required by legal process, and information authorized for release by clients.

Information that is protected under the following legislation must never be released unless required by law:

- Municipal Freedom of Information of Protection of Privacy Act (MFIPPA)
- Personal Health Information Protection Act (PHIPA)
- Personal Information Protection and Electronic Documents Act (PIPEDA)

### **Transmission by Email**

In most instances, confidential information should never be communicated via email. Employees authorized to reveal confidential information to another via email must specifically designate such information as 'CONFIDENTIAL' within their correspondence. Before revealing confidential information to outsiders, KDSB employees should ascertain whether outside law firms, banks, accountants and other outside consultants to whom confidential information may be given have confidential or "inside information" compliance procedures in place to guard against any misuse of such information by members of such firms.

### **Confidential Files**

Additional precautions should be taken when sending documents of a confidential nature. Employees who must transfer confidential documents via email are to ensure that the intended recipient is fully aware that the correspondence is 'CONFIDENTIAL'. Avoid using file names that might disclose confidential information.

Confidential files shall be password protected or encrypted. File protection passwords are NOT to be communicated via email correspondence in any event, and other arrangements are to be made for the disclosure of the password.

**Disclosure of Company News and Information**

Financial information about KDSB is not to be released to anyone unless it is included in a published report or otherwise made generally available to the public, usually through the company website or through official corporate communications, such as press releases.

**Media Inquiries**

All media inquiries regarding the company should be referred to the appropriate DEPARTMENT HEAD. The following subjects are never to be discussed with the media or in any public forum:

- Confidential business matters.
- Information about a client and the client's dealings with KDSB.

**Employee Information**

It is company policy to safeguard the confidential aspects of its relationship with its officers and employees; to satisfy all requirements of applicable labor laws; and to maintain uniformity in replies to inquiries concerning past and present officers and employees. In order to assure that this policy is consistently maintained, any request for information regarding past or present officers and employees must be referred to the appropriate DEPARTMENT HEAD. This includes salary verification, performance evaluation, or personal information (e.g.: address, social insurance number, phone number).

All requests for release of such information must be pre-authorized in writing by the officer or employee who is the subject of the inquiry.

## **Usage Guidelines and Etiquette**

**Email Best Practice Guidelines**

KDSB considers email an important means of communication and recognizes both the importance of well-worded messages and prompt replies where necessary to convey a professional image. Authorized Users must use good judgment in writing messages, in forwarding messages and attachments, or in reading email that was inadvertently sent to their mailbox. The following guidelines should be followed when using email:

- Authorized Users should review the content of their email communications prior to transmitting to make sure that the message is clear, has an appropriate subject line, and does not include information that might be misinterpreted by the recipient.
- Use the subject line to summarize the content of the email to enable recipients to interpret and prioritize the message quickly. This also enables the sender and recipient to locate archived messages speedily.
- Whenever possible, follow internal naming conventions as specified in record management policies to aid in the proper retention of messages.
- Email should not be drafted in capital letters, as this is more difficult to read and can be interpreted as shouting or yelling.
- Messages should be spell-checked before being sent.
- Mark messages as important only when they require urgent attention by the recipient.
- Use the 'cc' function to 'Carbon Copy' others sparingly. Consider whether it is really necessary to copy all recipients to reduce the volume of unnecessary email.

- Before planned leave or vacation, where email will be read only periodically or not at all, turn on Outlook's 'Out of Office Assistant' function clearly stating your dates of absence, whether email will be dealt with by someone else in your absence, and providing alternative contacts as required (note: this message should be worded professionally as it may be read by both colleagues and senders from outside KDSB).

### **Online Discussion Guidelines**

If an Authorized User uses his or her personal email address or Internet account to subscribe to any internet newsgroup, public forum, online discussion group or mailing list or creates a personal blog, he or she should not discuss corporate details or disclose proprietary or confidential information in any of those places.

Employees **MUST** obtain approval from the CAO before subscribing to online discussion groups such as Internet newsgroups, public forums and mailing lists using a KDSB email address.

Assuming that permission has been obtained, all postings by employees from a KDSB email address should include a disclaimer stating that views expressed are strictly their own and not necessarily those of the company, unless otherwise authorized.

### **Use of Portable Resources**

Laptops, notebooks, palmtops, portable digital assistants (PDAs), cell phones, cell phone/PDA combinations, pagers and other transportable information processing and communications devices are Electronic Communications Resources within the meaning of this Policy. Theft of these devices is a growing problem and, for the smallest and newest of these devices, no encryption products may be commercially available. Confidential information shall not be stored on portable resources unless encryption is used. Your responsibility is to ensure the availability and security of your portable Resources at all times.

Devices that are capable of storing company and customer data – such as laptops, notebooks, palmtops and PDAs – must be password protected. Devices that are highly transportable and easily lost shall only store copies of information with original data being downloaded onto the KDSB network.

Lock your portable devices in a desk drawer or cabinet prior to leaving the office or lock your office when away for an extended period of time or overnight (if you are not taking these portable devices with you). Care must be taken in reducing the possibility of loss of these devices both in the office and out. Your portable devices should not be shared; do not let others use them.

When traveling with these devices:

- Be aware of their locations at all times.
- Keep them secure. If you are staying in a hotel room that has a safe, consider placing them in the safe when you are out of the room and are not taking them with you.
- Do not leave them unattended, even for a moment.
- Keep them out of sight unless in use.
- Keep them on your person, in your briefcase or a separate PC carrying bag. Do not check these devices in airline luggage systems – they should remain in the traveler's possession as hand luggage.

KDSB may require transportable information processing and communications devices to be configured with the necessary controls and security features before being used for KDSB's business. It is your responsibility to check with the LSSC to determine if such devices need to be configured with such controls and/or security features. Be mindful that information may also be accessed visually in public areas thus this type of disclosure is prohibited.

**Remote Access and Use**

In certain circumstances, KDSB may permit certain Authorized Users to access the KDSB network and work remotely either generally or for temporary periods such as for medical reasons. In some cases the company may provide equipment or software to facilitate remote access. Authorized Users using a remote device or software not provided by KDSB to remotely access the KDSB network must have the same security features as a KDSB device before remote access is allowed.

The use of KDSB supplied equipment or software is restricted to Authorized Users only and it is the responsibility of Authorized Users to prohibit others from using such equipment.

All the supplied equipment and software and the information stored in them are Resources within the meaning of this Policy, and this Policy is intended to apply to them to the maximum extent that is physically and technologically possible.

Specifically:

- To the extent that these Resources have been supplied by KDSB they must be returned to KDSB or uninstalled immediately upon the request of KDSB or once employment is terminated.
- These supplied Resources must not be altered in any way (e.g., upgraded processor, expanded memory, or additional circuit cards) without the approval of the LSSC.
- Any exchange of KDSB data from a remote location with the KDSB network must be conducted using one or more security features or procedures approved by the LSSC.
- Authorized Users must report promptly any damage to or loss of any supplied Resources that have been entrusted to their care.
- Intellectual property developed or conceived while an employee is working at any remote location is the exclusive property of KDSB. This provision includes patent, copyright, trademark, and all other intellectual property rights as manifested in memos, plans, strategies, products, computer programs, documentation and other materials.
- KDSB maintains the right, with one or more days advance notice, to conduct inspections of the home office of any person who accesses the KDSB network from that location. KDSB may withdraw telecommuting privileges if it is not satisfied with the security arrangements in their remote location.

**Monitoring, Auditing and Access****Expect Monitoring, Auditing and Access**

KDSB has the right to monitor and audit all use of the Resources, regardless of where such Resources are located, and to access all files and messages stored on or processed through the Resources. Although the use of passwords and other forms of security are provided for the protection of KDSB information, no employee has, or should expect any, personal right of privacy with respect to any file or message contained within or processed through the Resources or with respect to any use of those Resources.

This Policy distinguishes between access and monitoring. Access involves opening and reviewing the content of files. Monitoring focuses on traffic patterns, general and individual levels of usage, file subjects and types, file origins and destinations, and network efficiency and security. It generally does not involve opening and reviewing the content of files. Auditing may involve both access and review of monitoring records, depending on the subject matter of the audit.

## **Purposes**

The Electronic Communications Resources may be monitored and audited, and the files on and processed through the Resources may be accessed, by authorized personnel for a number of purposes including maintaining and protecting the Resources for the benefit of KDSB compliance with law or, if necessary, undertaking the professional obligations of KDSB, ascertaining and helping to ensure compliance with KDSB's policies; and helping to ensure the proper operation of the Resources, including measurement of network traffic and investigation of suspicious circumstances.

## **Surveillance Software**

KDSB uses system software and software utilities (collectively, "surveillance software") to log, analyze and document use of the Resources and supervisors may receive reports generated by such software. The surveillance software may also be applied to transmissions with the KDSB network from remote locations and from portable devices.

## **Third Parties**

KDSB reserves the right to employ third parties to assist with monitoring and surveillance, including intrusion detection, "white hat" penetration and receipt of technological advice.

KDSB may use investigators who pose as other persons in order to test security policies or investigate alleged wrongdoing.

## **Extent of Monitoring**

### **Systematic monitoring allowed for any business purpose**

The company may engage in the systematic monitoring of electronic communications or other electronic files created by employees for valid business purposes, including employee supervision. All employees will be required to consent to such monitoring as a condition of employment.

## **Extent of Access and Disclosure**

### **Access or disclosure for any business purpose by those with authority**

Authorized managers and supervisors may access or disclose private electronic communications or files of an employee for any valid business purpose. Employees will be so required to consent to such access as a condition of employment.

## **Managing Email**

### **Removal of Email from Exchange Server**

#### **Automatic deletion after a certain period**

KDSB has implemented network procedures for periodically deleting emails from each Authorized User's mailbox as follows:

- a) Deleted Box – messages are deleted automatically upon sign out or after sixty (60) days, depending on how the Authorized User has configured his or her email software. The configuration that results in automatic deletion upon sign out is generally encouraged and is the default configuration on all new computers supplied to KDSB personnel.
- b) Normally, deletion as a result of network procedures will occur on a monthly basis.

**Request archived email from System Administrator**

KDSB has implemented a solution for archiving older email. To access email that has been removed from the KDSB Exchange Server, an Authorized User must send a request to the LSSC specifying which email is required.

## **Email Record Retention**

### **Default Retention Policy for Archived Email**

KDSB treats electronic communications as a business record. Business records are subject to federal and provincial laws as well as KDSB records management policies. This section is not intended to replace existing record retention policies and procedures but to enable its enforcement using an automated archiving solution that matches the classification and retention schedule outlined in the KDSB Record Retention Policy manual.

All electronic communications will be automatically archived for 5 years except for the following cases:

### **Human Resource Administrative Correspondence**

All electronic communication involving the Human Resource department that includes, though is not limited to, clarification of established company policy such as holidays, time card information, dress code, work place behavior, etc. shall be retained for 7 years.

### **Human Resource Employee-Related Messages**

All electronic communication involving the Human Resource department relating to employment contracts, background checks, occupational health and safety, employee complaints, etc. shall be retained for 7 years.

### **Fiscal Correspondence**

All information related to revenue and expense for the company shall be retained for 7 years.

### **Senior Management Correspondence**

All email sent by Senior Management shall be retained as required dependent on the subject matter.

### **Mergers and Acquisitions**

All communication related to mergers and acquisitions shall be retained for 7 years.

### **Legal Correspondence**

All electronic communication relating to legal issues such as trademark and intellectual property violations, sales contracts, business agreements, lawsuits, shall be retained for 7 years.

### **Corporate Audit Records**

All audit or review workpapers, and any correspondence which are sent or received in connection with an audit or review, shall be retained for 7 years from the end of the fiscal period in which the audit was concluded.

### **Auditor Correspondence**

All correspondence with or including the company auditors shall be retained for 7 years.

## Reporting Violations and Enforcement

### Reporting

Every Authorized User has a duty to report all suspected and known violations of this Policy and problems with the Resources to his or her immediate supervisor or to the LSSC on a timely basis so that prompt remedial action may be taken. This obligation includes reporting of any suspected malicious code.

### Unauthorized Users

Any use of the Electronic Communications Resources by any person who is not an Authorized User is strictly prohibited. Any such unauthorized use will be referred to appropriate governmental authorities for action and will be prosecuted vigorously by KDSB, regardless of whether such unauthorized use resulted in any loss to KDSB.

### Authorized Users

#### Discretionary in Management

Failure to conform to this Policy or any provision of it provides a basis for disciplinary action, which may include revocation of the privilege to use one or more of the Resources, dismissal without notice, in addition to any further disciplinary or other actions KDSB may deem appropriate.

The severity of the disciplinary action will depend on management's judgment as to the severity of the situation.

## **ACKNOWLEDGEMENT AND SIGNATURE**

### **Authorized User Acknowledgement**

When you have finished your review of the Electronic Communications Policy, you must agree that you have read the Policy, that you understand it, and that you are bound by and will abide by its requirements. You confirm these agreements by signing below. Failure to abide by the Policy's requirements may result in termination of your employment. If you have any questions at any time concerning the Policy, please consult your supervisor.

I agree that:

1. I have received an electronic copy of the Kenora District Services Board Electronic Communication Policy, dated as of \_\_\_\_\_.
2. As a condition of my employment, I am bound by and will abide by the Policy, any applicable supplements, and any additional or amended policies and procedures issued from time to time.

I understand that any violation of these Policies may subject me to disciplinary action, up to and including dismissal, as well as possible civil and criminal penalties.

\_\_\_\_\_  
Name

\_\_\_\_\_  
Date