

Toronto District School Board

Operational Procedure PR572

Title: **E-MAIL USAGE**
Adopted: June 28, 2000
Revised:
Reviewed: April 2012, **October 2012**
Authorization:

1.0 OBJECTIVE

To guide staff in the appropriate, legal and ethical use of e-mail provided by the TDSB to facilitate TDSB business.

2.0 RESPONSIBILITY

Chief Information Officer

3.0 DEFINITIONS

Compliance with this procedure is mandatory for all users of TDSB e-mail. E-mail access is intended for authorized business use and is not intended for private or personal communication. Staff found abusing the TDSB e-mail system and/or contravening the e-mail procedure will be subject to disciplinary action.

4.0 PROCEDURES

4.1. Usage

This procedure applies to all e-mail, which is accessed on or for from TDSB premises, using TDSB computer equipment, or via TDSB-paid access methods and/or used in a manner which identifies the individual with the TDSB. Messages or information sent by staff to one or more individuals via an electronic network are statements identifiable and attributable to the TDSB. All communication sent by staff via a network must comply with this and other TDSB policies and procedures and may not disclose any confidential or proprietary TDSB information.

E-mail is not secure and should not include message information that is private and confidential. It is not a confidential medium and is sent unencrypted and easily readable. E-mail is subject to monitoring by the TDSB for compliance with Board policies, rules and standards.

Users will:

- Use e-mail in a manner that will withstand public scrutiny and in compliance with existing Board policies and procedures, legislation, regulations, policies and standards, e.g. copyright, Intellectual Property Laws, Freedom of Information and Protection of Privacy Act.
- Use on-line services and resources efficiently and productively for the purpose of TDSB business only.
- Ensure the content of anything exchanged (sent and/or received) via e-mail is appropriate and consistent with TDSB policies, subject to the same restrictions as any other TDSB correspondence.
- Include a Records Classification System Code, where an e-mail message replaces a hard copy format and will be printed for the purpose of filing.
- Use the Microsoft Office format for all messages and attachments sent by e-mail.
- Ensure that confidential or proprietary TDSB information is not disclosed.
- Include an auto signature that contains methods by which others can contact the sender (department, title, phone number, fax number).

3.2 E-mail Guidelines

The purpose of the E-Mail Guidelines is to clearly communicate the Toronto District School Board's expectations of acceptable and efficient use of the e-mail communication system. These guidelines are intended to assist users communicate effectively and professionally.

Users will:

- Use e-mail efficiently and productively for the purpose of TDSB business only.
- Be courteous and follow acceptable standards of e-mail etiquette and will not propagate chain letters, jokes, cartoons, pornography or other e-mail debris when communicating on-line.
- Protect other's privacy and confidentiality.
- Keep messages short, brief and concise and use the attachment feature to forward large documents.
- Not use e-mail for urgent or emergency messages.
- Proof-read all messages.
- Store messages in folders rather than printing.
- Read and respond to messages daily, if possible, when in the office.
- Read and respond to messages every three days if absent from the office and use Out of Office Assistant to indicate when the messages will be read.
- Activate Out of Office Assistant with an extended leave message, indicating return dates, when absent for an extensive period of time.

- Be responsible for regular deletion of unnecessary e-mail.
- Be careful when using the Reply to All features in mail belonging to a mailing list, as these are sent to the entire list.
- Respond to a sent message by using Reply which maintains the thread of the original message and creates a link between the original message and the created response.
- Return, then delete any misdirected messages received that are intended for another person.
- Provide to their supervisor/manager any security measures for workstation passwords and encryption keys (if any) for TDSB use if required (e.g. there may be a need to access an employee's system or file when absent).