

DUFFERIN-PEEL CATHOLIC DISTRICT SCHOOL BOARD

GENERAL ADMINISTRATIVE PROCEDURES

Section: 300 – ALL STAFF
Procedure #: 316.00
Subject: **ELECTRONIC COMMUNICATION – USE AND REGULATIONS**
Reference: Policy 4.75
Effective Date: January 1, 2001
Revised/Amended:
Replaces: NEW
Page: 1 of 8

TABLE OF CONTENTS

- I. INTRODUCTION AND PURPOSE
- II. APPLICATION OF OTHER POLICIES
- III. SCOPE
- IV. SPECIFIC USE PROVISIONS
- V. INAPPROPRIATE USE
- VI. PERSONAL USE
- VII. CONFIDENTIALITY
- VIII. SECURITY AND PRESERVATION
- IX. VIOLATIONS

APPENDIX A: GENERAL USE AND CAUTION

I. INTRODUCTION AND PURPOSE

A. The within procedures clarify the applicability of law and of other Board policies/procedures to electronic communication, and also sets forth new procedures uniquely applicable to electronic communication.

B. The Board recognizes that principles of freedom of speech, privacy and confidentiality hold important implications for electronic communication and services. The within procedures address these principles within the context of, and subject to, the limitations imposed by the Board's legal and policy obligations.

The purpose of these procedures is to assure that:

- 1) Electronic communication will be used by the Board community in an ethical and considerate manner in compliance with applicable law and policies, including policies established by the Board and its operating units;
- 2) Electronic communication users are informed about how concepts of privacy and security apply to electronic communication, as well as the applicability of relevant policy and law; and
- 3) Disruptions to Board electronic communication and other services and activities are minimized.

II. APPLICATION OF OTHER POLICIES/PROCEDURES

- A. All other policies/procedures, applied generally at the Board, are also applicable to the electronic environment.
- B. Any policy/procedures which apply to the use of Board resources, including equipment and time, also applies to electronic communication. In the event of a conflict between policies, the more restrictive use policy shall govern.

III. SCOPE

- A. These procedures apply to:
 - 1) All electronic communication services provided, owned, or funded in part or in whole by the Board;
 - 2) All users and holders of Board electronic communication systems or accounts, regardless of intended use; and
 - 3) All Board electronic communication Official Records in the possession of or generated by Board employees and other users of electronic communication services provided by the Board, regardless whether the records were generated on Board or non-Board computers;
 - 4) Both internal and external electronic communication.
- B. The within procedures apply equally to transmission and receipt data including electronic communication headers, summaries, and addresses associated with electronic communication records and attached files or text.

IV. SPECIFIC USE PROVISIONS

A: Provision of Service

Electronic communication services may be provided by Board organizational units in support of the Board's mission.

B: Board Property

Electronic communication services are extended for the sole use of Board staff and other authorized users to accomplish tasks related to and consistent with the Board's mission. Board electronic communication systems and services are Board facilities, resources and property as those terms are used in Board policies/procedures and applicable law. Any electronic communication address or account assigned by the Board to individuals, sub-units, or functions of the Board, is the property of the Board.

C: Authorized Service Restrictions

1. Electronic communication users are required to comply with all applicable laws, Board policies/procedures, and normal standards of professional and personal courtesy and conduct. Access to Board electronic communication services is a privilege that may be wholly or partially restricted by the Board without prior notice and without the consent of the electronic communication user:

- a) when required by and consistent with applicable law or policy/procedures
- b) when there is sufficient cause or a reasonable suspicion that violations of law or policy/procedures have occurred or may occur; or
- c) when required to meet time-dependent, critical operational needs.

Such access restrictions are subject to the approval of the appropriate Board supervisory or management authority.

2. Board operational units may define additional "Conditions of Appropriate Use" for local computing to supplement this Policy with additional detail, guidelines or restrictions. Such conditions must be consistent with and subordinate to these procedures, and are intended to deal primarily with local situations.

3. When an individual's employment affiliation with the Board ends or is suspended, the Board may attempt to redirect electronic communication for a reasonable period of time as determined by the Board for purposes consistent with these procedures and the Board's mission. The Board may elect to terminate the individual's electronic communication account or continue the account, subject to approval, by appropriate Board supervisory and systems' operational authority.

D. Authorized Access and Disclosure

1. The Board may permit the inspection, monitoring, or disclosure of electronic communication when:

- a) Required by or consistent with applicable law, policy/procedures or any appropriately issued subpoena or court order;
- b) There is a reasonable suspicion that violations of law or Board policy/procedures have occurred or may occur; or
- c) There are time-dependent, critical operational needs of Board business.

2. In such circumstance, the Board may, inform electronic communication users prior to any inspection, monitoring, or disclosure of electronic records, except when such notification would be detrimental to an investigation of possible violation of law or Board policy/procedures. Users are required to comply with Board requests for access to and copies of electronic records when access or disclosure is required or allowed by applicable law or policy/procedures, regardless whether such records reside on a computer housed or owned by the Board. Failure to comply with such requests can lead to disciplinary or other legal action pursuant to applicable law or policy, including but not limited to appropriate Board personnel policies or Codes of Conduct.

E. Indemnification of the Board

Users agree, by virtue of access to the Board's computing and electronic communication systems, to indemnify, defend and hold harmless the Board for any suits, claims, losses, expenses or damages, including but not limited to litigation costs and attorney's fees, arising from or related to the user's access to or use of Board electronic communication and computing systems, services and facilities.

V. INAPPROPRIATE USE

A. Using electronic communication for illegal activities is strictly prohibited. Illegal use may include, but is not limited to: obscenity; hate literature, child pornography; threats; harassment; racial discrimination; theft; attempting unauthorized access to data or attempting to breach any security measures on any electronic communications system; attempting to intercept any electronic communication transmissions without proper authority; and violation of copyright, trademark or defamation law.

B. Theft or unauthorized destruction, mutilation, defacement, alteration, falsification, removal or secretion of electronic communication records may lead to legal and/or disciplinary action up to and including termination of employment.

C. In addition to illegal activities, the following electronic communication practices are expressly prohibited: entry, examination, use, transfer, and tampering with the accounts and files of others, unless appropriately authorized; altering electronic communication system software or hardware configurations; or interfering with the work of others or with Board or other computing facilities.

D. Board electronic communication services may not be used for:

- 1) Commercial activities, unless previously approved by appropriate Board supervisory authority;
- 2) Personal financial gain;
- 3) Personal use inconsistent with Section VI of this policy;
- 4) Uses that violate other Board policies/procedures or guidelines, but are not limited to, policies/procedures and guidelines regarding personnel, intellectual property, or regarding sexual or other forms of harassment; or
- 5) Uses that are inconsistent with applicable laws.

E. Electronic communication users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Board or any unit of the Board unless expressly authorized to do so. Where appropriate, the following explicit disclaimer shall be included: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion, or endorsement of the Dufferin-Peel Catholic District School Board."

F. Unless authorized, Board electronic communication services shall not be used for purposes that could reasonably be expected to cause, directly, or indirectly, strain on any computing facilities, or interference with others' use of electronic communication or systems.

Such uses include, but are not limited to, the use of electronic communication services to:

1. Send or forward chain letters, unsolicited material or communication to;
2. "Spam", that is, to exploit listservers or similar systems for the widespread distribution of unsolicited material;
3. "Letter-bomb", that is, to resend the same electronic communication repeatedly to one or more recipients.

VI. PERSONAL USE

Board electronic communication services may be used for incidental personal purposes provided that such use does not:

- A. Directly or indirectly interfere with the Board operation of computing facilities or services;
- B. Interfere with the electronic communication user's employment or other obligations to the Board;
- C. Violate these procedures, or any other applicable policy/procedures, or law, including but not limited to use for personal gain, conflict of interest, harassment, defamation of individuals, the Dufferin-Peel Catholic District School Board or its agents, copyright violation or illegal activities;
- D. Electronic communication messages arising from such personal use shall, however, be subject to access consistent with these procedures or applicable law. Accordingly, such use does not carry with it a reasonable expectation of privacy.

VII. CONFIDENTIALITY

A. The confidentiality of electronic communication is not guaranteed, and any confidentiality may be compromised by access consistent with applicable law or policy/procedures, including these procedures, by unintended redistribution, or due to inadequate technology to protect against unauthorized access. Users, therefore, should exercise extreme caution in using electronic communication to communicate

confidential or sensitive matters, and should not assume that their electronic communication is private or confidential.

B. Users may not access, use, or disclose personal or confidential information without appropriate authorization, and must take necessary precautions to protect confidentiality of personal or confidential information, regardless whether the information is maintained on paper or whether it is found in electronic communication or other electronic records.

C. The Board may elect to publish staff electronic communication addresses as directory information, consistent with the requirements of the Board.

D. Material is considered private and confidential when requested by the originator not to be forwarded to others.

E. Workplace privacy is not an absolute right and should not be an expectation of employees. Workplace privacy is balanced with the legitimate business interests of the Board.

VIII. SECURITY AND PRESERVATION

A. Electronic communication users and operators must follow sound professional practices in providing for the security of electronic records, data, applications' programs, and systems' programs under their jurisdiction.

B. Users are responsible for safeguarding their identification (ID) codes and passwords, and for using them only as authorized. Each user is responsible for all electronic transactions made under the authorization of his or her ID. Use of electronic communication user identifications for commercial purposes is prohibited. Access to user identifications may not be loaned or sold.

IX. VIOLATIONS

Suspected or known violations of policy/procedures or law should be confidentially reported to the appropriate supervisory level for the operational unit in which the violation occurs. Teachers must also comply with the "Teaching Profession Act, Regulation 18.(1)" and the "Ontario College of Teachers Act". Violations will be processed by the appropriate Board authorities and/or law enforcement agencies. Inappropriate use of electronic communication and/or violation of the policy/procedures regarding same could result in disciplinary action, up to and including termination of employment with the Board.

APPENDIX A

GENERAL USE AND CAUTION

Users should be aware of the following:

A. Both the nature of electronic communication and the public character of the Board's business make electronic communication less private than users may anticipate. For example, electronic communication intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. A reply to an electronic message posted on an electronic bulletin board or "listserver" intended only for the originator of the message may be distributed to all subscribers to the listserver. Furthermore, even after a user deletes an electronic record from a computer or electronic communication account, it may persist in whole or in part in system logs, in the directories of the person who received the message, or on system back-up tapes which may be retained for long periods of time. All these items may be subject to disclosure under applicable law and the within Procedures. The Board cannot routinely protect users against such eventualities.

B. Electronic communication, regardless whether created, received, or stored on Board equipment, may constitute an "Official Record"; may be subject to disclosure; or may also be subject to disclosure or access under other laws or as a result of litigation.

C. The Board does not automatically comply with all requests for disclosure, but attempts to evaluate such requests against the precise provisions of the applicable law and policy concerning disclosure and privacy.

D. The Board, in general, cannot and does not wish to be the arbiter of the contents of electronic records. Neither can the Board, in general, protect users from receiving electronic communication they may find offensive. Members of the Board community, however, are strongly urged to use the same personal and professional courtesies and considerations in electronic communication as they would in other forms of communication, and particularly those applicable to written communications since electronic communication creates a tangible record of that communication.

E. There is no guarantee, unless "authenticated" electronic systems are in use, that electronic communication received was in fact sent by the purported sender, since it is relatively easy, although a violation of these procedures, for senders to disguise their identity. Furthermore, electronic communication that is forwarded may also be modified. Authentication technology is not widely and systematically in use at the Board as of the date of these procedures. As with print documents, in case of doubt, receivers of electronic communication should check with the purported sender to validate authorship or authenticity.

F. Encryption of electronic communication is another emerging technology that is not in use as of the date of these procedures. This technology permits the encoding of electronic communication so that for all practical purposes it cannot be read by anyone who does not possess the right key.

G. Inappropriate electronic communication use may expose the Board and individual users to claims for damages through copyright infringement, libel, breach of privacy or other personal or proprietary rights.

H. Various laws and Board policies/procedures regarding copyright and intellectual property apply to electronic communication. Do not violate the copyright of others. Unless the material is legally established as being in the public domain or unless there is explicit release by the copyright owner, you may not copy electronic information. Under copyright law, you may or may not have copyright in electronic communication material which you create. Check with the appropriate authority before assuming that you have copyright in such material.

I. Even though an electronic communication sender and recipient have deleted their electronic record, back-up copies may exist for periods of time and in locations unknown to the originator or recipient. These copies may be accessed or disclosed consistent with applicable policy or law.

