

Policy:	EMAIL	FIN-501
Division:	FINANCE AND BUSINESS ADMINISTRATION	
Cross-Reference	<i>FIN-500 Acceptable Use of Technology</i>	

ADMINISTRATIVE PROCEDURES/REGULATIONS

1. General

- 1.1 Each Division is responsible for ensuring that employees and other users are made aware of policies and procedures/regulations regarding email use and management.
- 1.2 The NLESD will normally provide an email account to all employees, trustees, interns and others, as required, to be used in conjunction with their duties or activities with the NLESD. These accounts, denoted by the District's email domain name - **@nlesd.ca**, are centrally administered.
- 1.3 Users are responsible for complying with security measures in place and for the content they disseminate. The District's IT Department administers the security of the email system along with user authentication and access. Security measures applied are based on industry standards and practices. The IT Department also employs filtering software and other measures to protect systems from email containing viruses, to reject email from known SPAM senders and to scan inbound email for SPAM. However, the security and confidentiality of users' email records, and email transmission, is not guaranteed.
- 1.4 The NLESD employs various back-up and archival procedures. Systems are 'backed up' on a routine basis to protect system reliability, integrity and loss of data. Therefore, email messages may exist, despite being deleted by the sender and/or receiver.
- 1.5 Email messages that constitute records should normally be kept for at least **one year**, unless required to be kept longer in compliance with policy or legislation, at the direction of the Director of Education or for law enforcement purposes.
- 1.6 Email records retained in an individual's mailbox will be purged permanently from the email system after **three years**. Users are therefore advised to save any email records to be retained to a sub-folder or documents folder on a storage system other than the email server.

APPROVED: November 22, 2014
AMENDED: _____

EFFECTIVE: December 1, 2014

- 1.7 Email accounts that are not accessed for 400 days will be terminated and purged permanently from the email system, unless required for district purposes.
- 1.8 When an individual is no longer attached to the NLESD, it is the responsibility of his or her immediate supervisor to notify the IT Department that the email account is no longer needed. With respect to departing employees, this notification should be done via the Human Resources Division, as part of the employee exit process. This will ensure termination of a user's email account upon his/her departure.
 - a) Inactive employees (e.g. retiring, resigning) are responsible for ensuring that their email records and mailboxes are in order before they leave.
 - b) The NLESD is under no obligation to store or forward the contents of an individual's mailbox after s/he leaves.

2. Responsibilities of Users

- 2.1 Access to the email system is provided by entering a username and password. Each individual user is responsible for protecting the confidentiality of his/her email account and password information and for refraining from establishing the same password for personal purposes (e.g. access to home computer or personal email). Users must not attempt to gain unauthorized access to another person's email account.
- 2.2 Users are expected to be cautious when opening emails or attachments in order to prevent the spread of computer viruses. Emails from unknown sources should not be opened and should be immediately deleted. If a user receives a harassing or threatening email, s/he should retain the email for processing and notify his/her supervisor immediately. Email that is harassing, obscene, inappropriate or offensive should not be further distributed.
- 2.3 Individual email users are responsible for managing their own email accounts, including organization and cleaning (e.g. deleting transitory and personal emails), and complying with data storage quotas as set by the IT Department. Users are not permitted to store personal videos or photos in the email system.
- 2.4 The NLESD permits limited personal use of the email system by employees and other users provided such use does not:
 - a) Violate this or any other district policy;
 - b) Interfere with staff productivity;
 - c) Interfere with the business operations of the NLESD;
 - d) Interfere with IT operations or the email system; and/or,
 - e) Compromise the NLESD in any way.
- 2.5 Users are responsible for updating any website or conference created within the NLESD First Class email system, and for purging old data on a regular basis. Group distribution lists must also be updated at a minimum once per school year, by the person who initiated or requested the account.

APPROVED: November 22, 2014
AMENDED: _____

EFFECTIVE: December 1, 2014

3. Appropriate Use

- 3.1 Appropriate use of the District's email system includes, but is not limited to:
- a) Communicating with fellow employees, business partners of the NLESD, government departments and other public bodies, and members of the school community, within an individual's assigned responsibilities.
 - b) Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
 - c) Participating in approved educational or professional development activities.

4. Inappropriate Use

- 4.1 When using the NLESD email system, all users must comply with applicable federal and provincial laws. These laws include, but are not limited to, laws relating to defamation, privacy, copyright, harassment and child pornography. The email system must not be used to:
- a) Transmit any materials for illegal or unlawful purposes including copyright infringement, fraud, plagiarism, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
 - b) Access, store or transmit material that is offensive, objectionable, abusive, pornographic, obscene, sexist, racist, harassing, bullying or provocative, including adult-oriented content.
 - c) Solicit for personal financial gain and commercial purposes, or for conducting or pursuing one's own political, business or personal interests;
 - d) Promote any political party, candidates or election of any kind;
 - e) Distribute hoaxes, chain letters or advertisements;
 - f) Send, forward and/or reply to large distribution lists concerning non-school district business. This activity is considered a form of SPAM and is not acceptable.

5. Monitoring and Privacy

- 5.1 The email systems and other IT assets are owned by the NLESD and are therefore its property. Emails may be monitored or accessed by district personnel who are authorized to do so and have an appropriate reason for access, when:
- a) Required by and consistent with law, such as retrieving emails in response to a court order;

APPROVED: November 22, 2014
AMENDED: _____

EFFECTIVE: December 1, 2014

- b) There is reasonable justification that violations of law or of district policies have occurred;
- c) There is reasonable justification that email records contain information critical in meeting operational requirements of the NLESD.
- d) It is necessary to retrieve emails in response to an access to information request under the *Access to Information and Protection of Privacy Act*. In the event of an access request under ATIPPA, email holders may be informed that an email search will occur or has occurred.

5.2 Users are advised to use extreme caution when communicating personal or confidential information via email. Once an email is sent it becomes the property of the receiver and the sender loses control over the distribution. Users are also advised to double-check addresses; reduce c. c. and b. c. and reduce 'reply to all'.

- a) Steps should be taken to protect personal/confidential information to be transmitted by email, such as sending the minimal amount of information possible and masking personal identifiers (e.g. not including names). When sending an email outside of the NLESD email system, users are advised to encrypt sensitive information in an email or attachment.
- b) When using email to correspond, only board-owned email should be used to transact the business of the District.

REFERENCES:

Info-Tech Research Group: *E-mail Acceptable Use Policy (template)*
Government of Newfoundland and Labrador (Office of the Chief Information Officer):
Email Policy, Guidelines (2011-10-08), and Using Email Effectively
College of the North Atlantic: *Electronic email and internet usage.*

APPROVED: November 22, 2014
AMENDED: _____

EFFECTIVE: December 1, 2014