

NLSchools refers to all public K-12 English schools and school-related facilities under the jurisdiction of the Department of Education, Education Operations Branch and all employees working therein providing services and supports to such schools, including those who work in school facilities, student transportation, program implementation, student services, and procurement.

Policy Name

Email

Policy Statement

The Department of Education maintains an electronic mail (email) system to support communications; teaching and learning within NLSchools; and its business operations. All users are expected to use the system in a responsible, legal, and ethical manner.

Background

Email systems play a vital role in the information technology services infrastructure of the school system and is an essential mechanism for delivering educational programs and services and for managing administrative functions.

The use of the email system, like the use of other resources, is subject to normal requirements of ethical and legal behaviour. The purpose of this policy is to:

- Outline access privileges;
- Define expectations and responsibilities of users, and appropriate use of the email system;
- Protect the email system;
- Protect users; and,
- Safeguard information.

Scope

This policy applies to all employees, students, interns and third-party users of the Department of Education email systems and associated services operated by used within NLSchools. It applies to all @NLSchools.ca email accounts, temporary and permanent, all email accounts (both temporary and permanent) and all email records, regardless of the method of access and use (i.e. use of email via desktop and any wireless devices). It applies

to all those who have access to @NLSchools.ca email accounts including employees, students, interns and third parties.

Definitions

Email

Emails are messages created, sent and received between computers/terminals linked by communications facilities. For the purpose of this policy, email is inclusive of all items contained within the email account including, but not limited to: messages, invites and other calendar items, tasks, contacts, posts, notes, all attachments as well as system metadata. Emails are considered official government records. This would include transactions such as those approving or authorizing, delegating, making decisions and other similar transactions. These must be retained as official records of the government. A general guideline would be to save email records that contain information/documentation similar to what would be saved to a hard copy file/cabinet.

Transitory Email

Transitory emails may be deleted at the discretion of the originator and receiver. Transitory email records are only required for limited time to ensure the completion of a routine action or subsequent record. It does not provide evidence of a business activity, decision or transaction, OR it is a draft or duplicate and an updated or final version of the document has been produced. Therefore, it is not the official record of a government transaction or decision.

Terminated Account

Terminated email accounts are deleted from the email system and their contents are not able to be accessed. Terminated email accounts cannot be reactivated.

Personal Information

The [Access to Information and Protection of Privacy Act 2015 \(ATIPPA\)](#) defines personal information as information about an identifiable individual, including:

- Name, address or telephone number;
- Race, national or ethnic origin, colour, or religious or political beliefs or associations
- Age, sex, sexual orientation, marital status or family status
- An identifying number, symbol or other particular assigned to an individual
- Fingerprints, blood type or inheritable characteristics

- Health care status or history, including a physical or mental disability
- Educational, financial, criminal or employment status or history.
- Opinions of a person about the individual, and
- The individual's personal views or opinions, except when they are about someone else.

Policy Directives

1. Use of the Department of Education email system for NLSchools requires prior authorization of the Superintendent of Schools or designate.
2. All users are reminded that conduct via email may reflect on the reputation of government. Users are expected to treat email in a professional manner and to practice responsible use at all times. Users must ensure that they manage their email account in accordance with this policy and associated procedures as well as other policies including, but not limited to, the [Acceptable Use of Technology](#) policy, and all applicable federal and provincial laws. This includes when users participate in commonly shared collaboration areas such as conferences and workspaces.
3. The email system and other IT assets are the property of the Department of Education. The department reserves the right to restrict access to the email system without prior notice or consent, if there is reason to believe that violations of policy or law have occurred or when required to meet operational needs. The department does not routinely inspect or monitor email or internet usage. However, users should have no expectation of privacy in anything that they create, store, send or receive on the NLSchools email system.
4. The email system and messages may be monitored and/or accessed by personnel who are authorized to do so and have an appropriate reason for access. This includes monitoring email traffic and content for viruses and SPAM and investigating suspected misuse of email. The department may also be required to provide email messages for legal proceedings and in response to requests under the [Access to Information and Protection of Privacy Act](#).
5. Use of NLSchools email system may be revoked at any time for inappropriate use. Any use which violates federal or provincial laws and/or NLSchools policies may result in:
 - a) Loss of access privileges;
 - b) Disciplinary measures;
 - c) Termination of employment; and/or,
 - d) Legal action, including criminal prosecution.

Administrative Procedures

1. General

- 1.1 Each Division is responsible for ensuring that employees and other users are made aware of policies and procedures regarding email use and management.
- 1.2 The department will normally provide an email account to all employees, interns, and others, as required, to be used in conjunction with their duties or activities. These accounts, denoted by @NLSchools.ca email domain name are centrally administered.
- 1.3 Users are responsible for complying with security measures in place and for the content they disseminate. The NLSchools Information Technology (IT) Division 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 Division 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 IT Division 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 Superintendent of Schools 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.
- 1.7 Email accounts that are not accessed for 400 days will be terminated and purged permanently from the email system, unless required for NLSchools purposes.
- 1.8 When an individual is no longer attached to NLSchools, it is the responsibility of his or her immediate supervisor to notify the IT Division that the email account is no longer needed. With respect to departing employees, this notification should be done via the NLSchools Human Resources Division, as part of the employee exit process. This will ensure

termination of a user's email account upon their 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 department is under no obligation to store or forward the contents of an individual's mailbox after they leave.

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 their 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, they should retain the email for processing and notify their 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 Division. Users are not permitted to store personal videos or photos in the email system.
- 2.4 Limited personal use of the email system by employees and other users is permitted provided such use does not:
 - a) Violate this or any other NLSchools policy;
 - b) Interfere with staff productivity;
 - c) Interfere with the business operations of NLSchools;
 - d) Interfere with IT operations or the email system; and/or,
 - e) Compromise NLSchools in any way.
- 2.5 Users are responsible for updating any website or conference created within the NLSchools Google 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.

3. Appropriate Use

- 3.1 Appropriate use of the email system includes, but is not limited to:
- a) Communicating with fellow employees, business partners of NLSchools, other government departments, 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 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-related 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 Government of Newfoundland and Labrador and are therefore its property. Emails may be monitored or accessed by the NLSchools IT Division or other government

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;
- b) There is reasonable justification that violations of law or of NLSchools policies have occurred;
- c) There is reasonable justification that email records contain information critical in meeting operational requirements of NLSchools.
- 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 NLSchools email system, users are advised to encrypt sensitive information in an email or attachment.
- b) When using email to correspond, only department-owned email (@NLSchools.ca) should be used to transact the business of NLSchools.