Newfoundland & Labrador English School District

OFFICE OF THE DIRECTOR

Chair: *Goronwy Price*
C.E.O./Director of Education: *Anthony Stack*

TEN TIPS ON ATIPP*

Encouraging Good Privacy Practices in Your Workplace

1. OUR RESPONSIBIITY

The Newfoundland and Labrador English School District and all of its employees are responsible for the protection of personal information about individuals within the custody and control of the District.

2. THEIR INFO/YOUR INFO

When working with personal information, make sure to handle it in a sensitive and confidential manner. Treat other people's information the way you would like to have your own personal information treated in any organization you deal with....for example, your bank or medical clinic.

3. ACCESS TO INFORMATION

Information/records generated through the course of your work may be "ATIPP-able" and, upon request, may be released in full or in part in response to an access to information request. Be mindful of this when making notes and sending correspondence.

4. EMAILS ARE ATIPP-able

Emails are considered NLESD records, and as such may be released in full or in part in response to an ATIPP request. Always treat your email professionally and follow the NLESD Email Policy, posted to https://www.nlesd.ca/about/policies.jsp, when sending and receiving emails.

5. MINIMIZE IDENTIFYING INFORMATION IN EMAILS

It is very easy to accidentally send an email to the wrong person. We have all done it! It is also worth noting that when you send an email, you lose all control over its distribution. To reduce the risk of a privacy breach, minimize the amount of personal and identifiable information contained in email. Best practice is to depersonalize information and, for instance, use a file number or initials to refer to an individual or encrypt the information in an attachment. Keep the email as short as possible and reduce c.c., b.c. and 'reply to all'.

6. PROTECT YOUR PASSWORD

Information Technology security precautions are in place for a reason. Make sure you protect your password, follow the security restrictions that are in place and remember to log off/lock your computer when you are not in your office.

7. LOCK IT AWAY

Leaving files that contain personal or confidential information out in the open is not good practice. Active files that you are working on should not be left on meeting room tables, in open offices/cubicles or on printers or copiers. Make sure information is stored safely away in a locked cabinet and/or locked office.

8. DO NOT LEAVE INFO UNATTENDED IN VEHICLES

A common form of privacy breach is the theft of briefcases or mobile devices (e.g. laptops) from vehicles. If it is necessary to carry sensitive personal information outside of the office, only take the minimum amount of information necessary for the task at hand, encrypt information that is contained on electronic devices and do not leave the information unattended in a vehicle.

9. SHRED IT

When it is appropriate to dispose of information, make sure you shred hard copy documents containing personal or confidential information in a manner that prevents them from being read or reformatted.

10. USE SOCIAL MEDIA RESPONSIBLY

Social media platforms such as Twitter, Instagram, YouTube, etc. provide great ways to connect with others and share information. However, there are pitfalls associated with social networking. Be mindful that information posted to a social networking site may be considered public information. Never post information about others to such a site without their permission.

** For NL Access to Information and Protection of Privacy Act click here: ATIPPA*

Updated: NLESD January 2017

95 Elizabeth Avenue · St. John's, NL · A1B 1R6
Tel: (709) 758-2372 · Fax: (709) 758-2706
www.nlesd.ca · @nlesdca