OFFICE OF THE ASSISTANT DIRECTOR
(Finance & Administration)

Chair: *Milton Peach, B.A., B.A.(Ed.)*
C.E.O./Director of Education: *Darrin Pike, B.Sc., B.Ed., M.Ed.*

DIRECTIVE

To: Eastern School District – All Schools

From: Eric C. Snow – Assistant Director of Education
Finance and Administration

Date: December 1, 2008

Subject: Secure Data Transportation - Encryption

Secure Data Management

The province of Newfoundland and Labrador proclaimed privacy legislation in January 2008, specifically the privacy portion of the Access to Information and Protection of Privacy (ATIPP) Act. This Act governs how public entities collect, protect, and use personal information. Consequently the Eastern School District is working to be ATIPP-compliant with respect to the information being processed. The work culture of the K-12 environment is such that teachers commonly transport data outside school facilities, sometimes working at home on a privately owned computer system. We realize that it is important to maintain the flexibility to access work information outside of school facilities and beyond normal school hours. As a result, a provincial committee of all public education stakeholders - the Provincial Education Protection of Privacy Committee - was formed to develop policies and procedures that reflect the appropriate balance of security and practicality with respect to data being worked on by teachers and school administrative staff.

Our goal is to support teachers and school administrative staff in carrying out their work assignments, while at the same time promoting secure working conditions for the protection of personal and confidential information.

Secure Data Transfer - Encryption

Personal storage devices, such as USB flash drives, are more powerful than ever and have become an ever-present tool in our education system. However these devices are also easily lost, possibly leading to personal information being exposed (a “breach”). These concerns lead us to understand that new policies and technologies must be implemented toward protecting information being stored on personal storage devices. The modern-day standard for protecting information is “encryption”; essentially scrambling the information so it is inaccessible if the drive is lost. Most drives being used by teachers were not encrypted, thus we have supplied new drives

with built-in encryption to schools. Alternatively, software can be used to encrypt normal drives. In addition to encrypted USB drives, the FirstClass messaging system supplies a secure method of transporting information, with no requirements for any special devices. Therefore, to help ensure the security of personal and confidential information during data transfer, one of the following two options ***must*** be used to transfer personal and confidential information data between computers at school or workplace and your home computer or alternatively to another computer system:

1. **FirstClass**: The File Storage feature (upload and download) of FirstClass offers a secure and encrypted technique to move data between school computers and home computers. Using the FirstClass client, data can be uploaded and downloaded as a means to transport data from school to home and back again. Attached is a short *User Guide* that explains the file transfer process using FirstClass.

   Please note that the data is secure and encrypted when uploaded to FirstClass. When you download the file and open it on your home computer, the data is no longer protected and is only as secure as the security features (e.g. AntiVirus) that you have installed on your home computer. After processing, data should be uploaded to the FirstClass system by using the file transfer method (*User Guide*) noted above and then deleted from your home computer system, including the Recycle Bin.

2. **Encrypted Media**: Encrypted memory sticks (jump drives, USB drives, etc.) must be used to transport personal and confidential information. Two options are available:
   - MXI Security encrypted USB drives (Government Standing Offer)
   - Software encrypted USB drives (TrueCrypt). The District has software that can be used to encrypt data on existing (unencrypted) memory sticks and hard disk drives.

   Please contact a District IT Technician in your region for assistance to add the encryption software to your memory stick or hard disk drive or to obtain an MXI Security encrypted USB drive.

   Please note that the data is secure and encrypted when it is located on the encrypted USB device. When you *download* a file and open it on a computer, the data is no longer protected and is only as secure as the security features (e.g. AntiVirus) that are installed on the computer system. After processing, data should be copied to the encrypted USB device and then deleted from the computer system, including the Recycle Bin.

BEST SECURITY PRACTICE: When using an encrypted jump drive, USB drive, etc. do not copy data to the local hard disk drive for processing, but instead work directly from the encrypted device. This process will avoid data inadvertently being downloaded and left on a local hard disk drive after processing.

At present time we are striving to eliminate the use of *unencrypted* storage devices for use with personal and confidential information. Encrypted storage devices (e.g. USB Drive, Flash Drive, Thumb Drive, Jump Drive) are currently being deployed. As well, implementation of TrueCrypt is also available which can be used to encrypt an unencrypted device. Our goal at this time is to provide a secure means to transport sensitive data while at the same time raise awareness in the protection of personal and confidential information.

We acknowledge that additional examination of current work practices will be required, beyond these security measures, to further ensure the protection of personal information and to meet our obligations under the *Access to Information and Protection of Privacy Act.* Further procedures and directives will be developed and circulated regarding security provisions for transporting personal and confidential information.

Thank you, in advance, for your cooperation on this very important matter.

ERIC C. SNOW, CGA
ASSISTANT DIRECTOR OF EDUCATION
(Finance & Administration)

ECS/ms