

### Software Piracy and Care

Unauthorized duplication of copyrighted software is illegal and is against District policy.

- Do not use unlicensed, unauthorized software on District computers..
- Software CDs and Documentation should be stored in a locked desk or cabinet.
- Backup copies of all software should be made and stored properly.
- Inventory records should be kept of all software..

### Acceptable Use Policy

It is acceptable to use the Internet service to gather information that is of value to the education process, for professional development and for communicating with people involved in the education system.

It is not acceptable to use the Internet for unethical or illegal purposes. Inappropriate use for access to inappropriate sites, includes, but not limited to , gambling, offensive images, videos, text, etc. that can be considered obscene, criminal, defamatory, violent, harassing or hateful..

### Violation Reporting

If you suspect tampering with your workstation or access ID please notify your principal or supervisor or call a technician assigned to your zone..

### Security Message

The Labrador School District has many computer networks which house personal and confidential information about our students, teachers and other that play a part in the education process. We also have “corporate” Information that is necessary for the “business” side of education. This information is essential to our operations and must be handled by each of us in a secure and confidential manner. Our Ability to achieve a secure operation requires a commitment to security by everyone.



**LABRADOR**  
DISTRICT SCHOOL BOARD

## Responsible Computing



**LABRADOR SCHOOL BOARD**  
[www.lsb.ca](http://www.lsb.ca)

When we speak of security, we are usually concerned with the protection of our personal belongings. We lock our doors, cars, desks, etc., to ensure the safety of our assets.

Yet many of us are unaware of the steps we should take to protect our information assets stored on the District's computers systems. This pamphlet was developed to provide a guideline to help secure one of our most valuable assets-our data!

### Access IDs

All employees (educators and support staff) receive a user ID and password to access the information systems they have been authorized to use.

- Do not share your User ID. Each person is accountable for the use of his or her User ID.
- Principals and supervisors must notify the IT department when a User ID is no longer required.

### Passwords

The password is critical to system security. It is the key to accessing the system and its data. Therefore, it should be kept confidential. All employees are responsible for the confidentiality of their passwords.

To assist in keeping passwords confidential it is necessary to create secure passwords, i.e., passwords that cannot be easily guessed or cracked. We suggest that passwords be made up of two smaller words with its letter scrambled or a character inserted in it, or a word misspelled.

Avoid creating passwords which can easily be associated with the owner such as family or pet names, dates or holidays.

Cracker programs can crack passwords in minutes if the password is found in the dictionary or is a name.

The District has established a standard for passwords:

- Passwords must be 8 characters in length and use a combination of alpha-numeric characters..
- Passwords will expire every 90 days and you cannot use any of the previous four passwords.
- Dictionary words must not be used.

Avoid writing down passwords. Passwords should be committed to memory. If you have to write it down, store it in a very secure place.

### Workstation Usage

Logoff computers at the end of each day. When leaving your computer unattended, even for a short period of time, use the Ctrl\_Alt-Delete function to lock your computer

Understand the various network storage areas (servers) and drives available for your use. This will enable you to store data in the appropriate location on a server. It is not appropriate to store private and confidential information on your C: drive.

### Laptop Usage

- Laptops must be secured to stable objects with a security locking cable to assist in preventing laptop theft.
- Store personal and/or confidential data on a server, or network drive or encrypted external drive.
- Please insure that your laptop is encrypted
- Do not leave your laptop unattended in open view. Always lock your laptop with the Ctrl\_Alt-Delete function whenever it is left unattended and make sure it is secured with a locking cable

### Printed Documents

- Label reports, documents and faxes containing sensitive information as RESTRICTED or PRIVATE.
- Seal any sensitive information that is sent through the postal service or courier
- Sensitive reports should be stored in locked cabinets.
- When Faxing personal and/or confidential information ,ensure the recipient is waiting for your fax and has received it

### Viruses

Computer Viruses are very common in the workplace. They result in lost data and productivity. The key to controlling the damage caused by viruses is by continuously running a valid and updated anti-virus program.

- The District has anti-virus software available for use on all District-owned computers. Make sure it is operating on your school/office computers and it is being updated automatically.
- When downloading files scan them for viruses immediately.
- Do not run unknown executable files on your computer. Contact the IT Department if you are not sure of the source of the executable file.
- If you Suspect you have a virus, stop using your computer immediately and call the IT Department. Do not shutdown your computer .Make notes of the last commands you have keyed and the messages you have received. Call the IT Department.