COMMUNITY LIVING
Thunder Bay

Number: FIN 10.0
Date: March 2011
Supersedes: n/a

GENERAL MANUAL POLICY

APPROVED BY: K. J. Pickard
Executive Director

CATEGORY: Finance

TOPIC: Computer Use

POLICY

Community Living Thunder Bay provides its users with computer/internet access and electronic communications services as required for the performance and fulfillment of job responsibilities. These services are for the purpose of increasing productivity and not for non-business activities.

PURPOSE

The purpose of this policy is to communicate user responsibility and clarify what is considered to be acceptable use of CLTB information technology (IT) resources.

SCOPE

IT resources include personal computers, workstations, file/database/application/e-mail /web/print servers, network resources, connections to these networks, services offered over these networks, all forms of software, all related peripherals and communication infrastructure including company supplied cell/smart phones.

EXISTING LEGAL CONTEXT

All existing laws (federal and provincial) and CLTB regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

PRIVACY

All computers and information technology systems provided to employees are owned solely by CLTB and are not the employee's property. All information created on the CLTB computer systems or network or as part of the job function of a CLTB employee is considered to be the intellectual property of CLTB and is not considered to be within the private domain of the user.

Employees have no right to expect that their files, e-mails and other data will be kept private. CLTB may at any time monitor computer/network usage and emails for purposes of security, network maintenance and to verify compliance with the policy. Should you have highly confidential information stored on your computer, please advise the System Administrator of said information at the time of a service request.

Monitoring of Computer and Internet Usage: CLTB has the right to monitor and log any and all aspects of its computer systems including but not limited to: monitoring internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.

Blocking Sites with Inappropriate Content: CLTB has the right to utilize software and/or hardware that makes it possible to identify and block access to internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

ACCEPTABLE USE OF E-MAIL

Community Living Thunder Bay e-mail accounts are not to be used to create or forward any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability or are or could be interpreted as being intimidating, harassing, unlawful, or containing hostile, degrading, pornographic, or otherwise offensive references.

The e-mail system should not be used to send or receive large attachments (i.e. video files). These files take up a large amount of space on our e-mail server and take a long time to upload and download. Should you have a need to send or receive large files for work purposes, please see the System Administrator and they can set up an alternate method for this.

Forwarding of e-mail chain letters using CLTB e-mail addresses is forbidden, as these are often used to collect e-mail addresses that are then added to unsolicited e-mail (spam) lists. Should you receive an e-mail about a potential virus / computer security issue you believe to be legitimate, it is to be forwarded to the System Administrator for verification, and he/she will send it out to all users after it has been verified as truthful.

All staff that are assigned a corporate e-mail address must check their email account on a regular basis, either on every shift or as instructed by your immediate supervisor. For those employees

with an "@cltb.ca" e-mail address using Microsoft Outlook, for absences of 5 work days or greater, it is required that you set an "out of office" auto-reply on your e-mail account.

All CLTB related e-mail is to be sent though CLTB email accounts. Personal e-mail accounts are not to be used for any CLTB related activity.

Users should be aware that e-mail is not a secure form of communication and that an alternative method of transmission should be considered for highly confidential data.

ACCEPTABLE USE OF THE INTERNET

Occasional and reasonable personal use of the internet is permitted, provided that this does not interfere with work performance and is used in an acceptable manner.

Violations of acceptable internet use includes, but is not limited to, accessing, downloading, uploading, saving, receiving, or sending material that includes copyrighted material (i.e. music/software), sexually explicit content, racial slurs, gender-specific comments or any other material that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability or are or could be interpreted as being intimidating, harassing, unlawful, or containing hostile, degrading, pornographic, or otherwise offensive references. Users should not use the internet services provided to disclose corporate or information related to people supported without prior authorization. Gambling and illegal activities are not to be conducted on company resources.

Should you accidentally be exposed to such content while using the internet (via popup ad, banner advertising, deceptive link, etc.) please alert the System Administrator so they can investigate your machine for a possible spyware infection.

SCARCITY OF RESOURCES

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending non-business related mass mailings or chain letters, spending excessive amounts of time on the internet, storage of personal files (i.e. pictures/music/videos) on CLTB servers, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files (i.e. web-based radio stations or You Tube), or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the internet.

Priorities between uses (i.e. data processing versus research versus system maintenance) and between users (i.e. employees in different locations and job classifications) will vary from system to system and according to time of day, week and year.

All email communications should be routinely and regularly deleted from the in-box, sent items box and trash bins so resources are not tied up in storage of excessive materials.

HARDWARE / SOFTWARE

All users of computer resources of CLTB must take care in the treatment of all IT hardware. Users are not permitted to physically abuse CLTB equipment or attempt to render the system or equipment inoperative, including careless use leading to damage or destruction.

Improper installation of hardware / software can result in unexpected computer behaviour. All hardware and software installation on computers owned by the organization is to be approved and performed by the System Administrator. This policy applies, but is not limited to, external storage devices ("USB keys"), portable music / video players, electronic organizers (Palm Pilots, Pocket PCs), digital cameras, etc.

No software copy is to be made by any user without a prior, good faith determination that such copyright is in fact permissible. All users must respect the legal protection by copyright and license to programs and data.

A standard array of software is installed for all computer users in the organization. Should you require additional or specialized software, please see the System Administrator.

CREATION OF ACCOUNTS

Should new staff require computer logins / e-mail addresses, their supervisor is to put a request in with the System Administrator at least 2 days prior to their first day of work. This ensures enough time to set up the appropriate level of access and computer orientation for the employee. This also applies to staff changing positions which may require a change in network permissions and/or access to new/different resources in the performance of the new role.

VIRUS DETECTION

Files obtained from outside sources, including disks brought from home, files downloaded from the internet, newsgroups, bulletin boards, or other online services, files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that can cause damage to the computer network. Users should never download files from the internet, accept e-mail attachments from outsiders, or use disks from non-Company sources, without first scanning the material with approved virus checking software. If you suspect that a virus has been introduced into the network, notify System Administrator immediately.

Disabling or attempting to disable installed antivirus/firewall software is considered to be a violation of this policy. If the antivirus/firewall software poses a problem contact the System Administrator immediately.

GENERAL MANUAL PROCEDURE

TOPIC: Computer Use

SECURITY

All employees are responsible for the accounts that are given to them by CLTB. This includes data backup where applicable and password maintenance.

1) Choose a password that cannot be easily guessed by others. Do not use your birth date, children's names, or other information that coworkers may be aware of.

2) Passwords must be maintained as follows:
   a) Passwords must be changed every 90 days
   b) Passwords will be at least 6 characters in length
   c) Password must meet complexity requirements, this means that all passwords must meet 3 of the following 4 requirements
      1) Must have one upper-case letter
      2) Must have one lower-case letter
      3) Must have one number
      4) Must have one non alpha numeric character (i.e. ! @ *)

3) Employees that suspect that their computer has been accessed by an unauthorized person should contact the System Administrator immediately.

4) The System Administrator is responsible for the overall security of the CLTB network. Employees should not however assume that information that they access or create is private. Employee's accounts may be accessed at anytime for maintenance, servicing or troubleshooting of the system, or as part of an investigation into misuse or abuse of the CLTB computer systems or network.

5) Do not leave your computer unattended without locking it. Press CTRL-ALT-DEL and select lock this computer or press insert the windows key symbol? Windows key and the 'L' key simultaneously.

6) The direct supervisor of any employee whose CLTB employment has ceased is responsible for informing the System Administrator at least 24 hours prior to employees last day of work so that the account may be disabled for security purposes.

7) The direct supervisor of any employee on an approved leave of absence is responsible for informing the System Administrator at least 24 hours prior to the employees last day of work to allow the account to be temporarily disabled and email to be forwarded to the appropriate individual.

PROHIBITED USES OF COMPUTER/NETWORK RESOURCES

1) Violations of laws including federal, provincial or local laws or CLTB policies
2) Offenses against others including, but not limited to:
   a. Harassing another via the computing and network facilities

b. Impersonating another
c. Taking or altering another's work without permission
d. Interfering in another's legitimate use of computing and network facilities
e. Displaying obscene material in a public area. Any direct attachment, linkage or anchoring of such materials to document viewable by the public is prohibited

3) Abuse of accounts including, but not limited to:
   a. Attempting to gain another user's password or to log on as another user
   b. Using an account for commercial purposes, except as authorized by CLTB. Users must be aware that it is against the policy of the CLTB to engage in activities concerning outside employment
   c. Deliberate alteration of the account structure assigned to the user so as to increase system permissions
4) Abuse of equipment or services including, but not limited to:
   a. Attempting to render the system or equipment inoperative
   b. Participating in activities which have the intent of tying up computing and network resources
   c. Physically abusing CLTB equipment
   d. Theft of CLTB equipment
5) Personal use of equipment or services including, but not limited to:
   a. Excessive or unauthorized personal use of company resources including e-mail, internet, data storage, etc.
   b. Damaging the reputation of the Association by creating, viewing, storing, transmitting, sending, or intentionally receiving communications, files, or documents that are or could be interpreted as being intimidating, harassing, unlawful, or containing hostile, degrading, sexually explicit, pornographic, discriminatory or otherwise offensive references
   c. Use of CLTB computing and network resources for one's own business endeavours, including the creation or circulation of personal resumes to outside organizations

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment. Referral to police agencies may be made in the case of suspected law violations.

POLICY REVIEW

This policy will be reviewed on an annual basis to account for technology changes and changes in CLTB planning.