Acceptance Date:	**November 23, 2004**	Resolution #:	**04-150**	Reference #	**BPL-04-05**
Revision Date:	**June 21, 2006** **June 26, 2007** **June 22, 2010** **January 12, 2012** **August 1, 2012** **November 26, 2013**	Resolution #:	**06-65** **07-72** **10-22** **No Change** **No Change** **No Change**		

BRAMPTON LIBRARY

Information Technology Use Policy

Policy Statement

The Library's information technology environment greatly increases our ability to adapt technology to business needs across the Library. For this policy, the term employee refers to all full and part-time employees and any other authorized persons who have access to information technology or who are in the process of receiving access. The technology allows employees to communicate with others and share information and peripheral devices.

The Library requires employees to use information technology in a professional, ethical manner, in accordance with the Library's obligations under Privacy legislation and to best service the business requirements of the Library. Failure to comply with this policy may result in loss of privileges and/or disciplinary action up to and including dismissal, depending on the severity of the infraction.

The Information Technology Use Policy provides clear and comprehensive guidelines for the use of personal computers, applications, Internet and e-mail.

The policy has been put in place to protect the Library and its information technology infrastructure against unauthorized access, legal liability, misrepresentation, release of confidential or proprietary information, inappropriate use, threats to the integrity of the infrastructure and to protect the Library's information technology and data assets.

Purpose

This policy is intended to protect the Library and its information technology infrastructure against hazards such as:

- unauthorized access,
- malicious manipulation and/or destruction of information/data,
- virus invasion,
- inappropriate use,
- litigation due to misappropriation of software and/or data,
- and/or inappropriate disclosure of personal information.

Compliance with the policy will also ensure data integrity and security and prevent employees from using technology to misrepresent the Library.

Scope

This policy applies to anyone who either directly or remotely has access to the Library's information technology infrastructure, applications, files and e-mail or any other technical services or peripherals.

Policy Format

Section 1 - Accountability
Section 2 - Common Practices provides information that is relevant to all of the sections of the policy.
Section 3 - Personal Computer Policy
Section 4 - Policy for the Use of Corporate Applications
Section 5 - E-mail Policy
Section 6 - Internet Policy
Section 7 – Administration

Section 1 - Accountability

1.1 Ownership

All computer equipment, licensed versions of software programs, and electronically created files and e-mails are considered the property of the Library. Library property should not be defaced in any manner. This includes but is not limited to attaching decals to computers, engraving initials, etc.

1.2 Responsibilities

All employees are expected to use good judgement, demonstrate a sense of responsibility and must comply with the policy when using Library computer equipment. All employees are required to sign a copy of the Information Technology Use Policy acknowledgement form after reading and understanding the policy.

In order to protect the interests of the Library and employees, it must be understood that any information relating to intrusions (hacker attacks) or even rumors of breach of our security should be reported to the Helpdesk.

All supervisors up to and including the CEO are required to ensure all employees receive, understand, comply with the policy and enforce the policy.

Library Systems staff will be responsible for monitoring and reporting infractions. Library Systems is also responsible for reviewing and updating the Information Technology Use Policy on an annual basis.

If one employee uses another's computer equipment (not login), during vacation or leave of absence, the system should be returned to its original configuration of the employee's upon return to work.

1.3 Personal Use

Incidental use of information technology for personal use is acceptable, provided the privilege is not abused. Examples of inappropriate personal use are spending lengthy periods of time, use for profit, or use that would otherwise violate the policy with regard to employee time commitments or Library equipment.

1.4 Computers

Shared computers may be necessary. In such situations a shared computer will be provided and is the responsibility of the immediate supervisor to ensure those employees sharing the computer comply with the policy. Shared computers will require employees to use application authentication as required to perform their job duties. Shared computers will allow no customized configuration by the employee.

Employees, where applicable, will be provided a computer. Library Systems will provide appropriate physical security such as cable locks for the employee to use. Employees are responsible for the security of their passwords.

No personal computing equipment, storage or other devices may be connected into the Library Corporate Network. No use of personal computing equipment, storage or other devices may be used during an employee's hours of work.

1.5 Inappropriate Use and Inappropriate Material

In this policy, "Inappropriate Use" means using the Library's information technology for, but not limited to:

- personal use other than as set out in subsection 1.3,
- creating, accessing, sending, uploading, downloading, posting, loading or saving inappropriate material,
- creating, sending, uploading, posting or loading information that constitute threats, harassment, libel, slander, defamation or other similar acts,
- creating, sending, uploading, posting or loading information that constitutes a nuisance, including spamming and virus distribution; and any other use prohibited by this policy.

"Inappropriate Material" means, but not limited to:

- any pornographic or violent material including text and pictures,
- hate propaganda,
- other material prohibited under legislation and Library policies.

Section 2 – Common Practices

This Section makes reference to information that is common to all sections of the Information Technology Use Policy.

2.1 Security

Library Systems is responsible for the security and integrity of the Library's computing environment. Network and computer access is facilitated by Library Systems, following the Library's guidelines and procedures.

2.2 Personal Information

Personal information refers to recorded information about an identifiable individual and includes information recorded via electronic means. Personal information should not be collected, used or

disclosed except in accordance with the *Municipal Freedom of Information and Protection of Privacy Act.*

In addition to monitoring employee's internet usage, e-mail, file storage and corporate computer configurations as described in subsection 2.4 below, the Library may collect and store this information. The *Municipal Freedom of Information and Protection of Privacy Act* authorizes the collection of this information. The information is to be used for the purposes set out in the Policy Statement and Purpose in sections 1.1 and 1.2.

2.3 Virus Protection
To ensure our computing environment remains virus-free all approved software shall be acquired from an authorized vendor. Files obtained through any means must be scanned for protection prior to installation. If a virus is detected, contact the Helpdesk immediately to ensure appropriate measures are taken to protect the overall computing environment.

2.4 Monitoring
Utilities are in place to monitor access, security threats, vulnerabilities, data, email and storage usage and Library network \ computer equipment configurations. Library Systems reserves the right to filter, block or restrict the use of unauthorized software.

The Library, through Library Systems, may monitor an individual's information or electronic data to ensure appropriate use. Monitoring will also assist in protecting the security of the Library computing environment.

By way of this policy, Library Systems is also fully authorized to review former or current employee information (i.e. e-mail, files, Internet access) without notice at any time as required to meet legal obligations.

It is understood that members of senior management deal with highly confidential issues on a regular basis, and can be deemed a "confidential group". In the event that the monitoring tools identify a potential threat to our environment, and the e-mail and/or document in question is to/from a member of the "confidential group", then the information will only be accessed by the Technology Manager or designate for the purposes of security.

2.5 Enforcement
An infraction notification process has been put in place to address non-compliance with the policy. It will be the responsibility of the employee’s Manager to determine the appropriate response to infractions.

Failure to comply with this policy may result in loss of privileges and/or disciplinary action up to and including dismissal, depending on the severity of the infraction. All disciplinary action will be in accordance with the Library's processes.

In the event that equipment/software appears to be maliciously damaged or if a violation of the policy occurs, any costs incurred will be the responsibility of the employee.

2.6 Access
Each employee's password must be confidential. The employee should not share his/her password with anyone or leave it where someone else could access it. The network system requires employees to change their passwords on a regular basis.

2.7 Account Management
Managers are responsible for informing Library Systems immediately when staff have been transferred, have a name change, are absent from work for four weeks or more, have been terminated, or when a temporary or alternative staff requires access to another individual's account or files.

2.8 Inappropriate Material
No employee shall store inappropriate material in any form on the Library's computer equipment. No employee shall access, upload from or post to websites inappropriate material, send inappropriate material through e-mail, or bring in inappropriate material for loading on the Library's computer equipment.

2.9 Records Retention
All information created or stored on the computer or transmitted through e-mail are documents in the custody and control of the Library and are subject to the *Municipal Freedom of Information and Protection of Privacy Act* and the Library's *Records Management Policy.*

2.10 Further Information
For more information regarding the policy please contact the Helpdesk.

Section 3 – Computer Policy

Please ensure that you also review Sections 1 and 2 which also contain guidelines on computer use.

3.1 Introduction
The Library’s information technology infrastructure allows employees access to an extensive network and productivity tools via the computer.

Each computer has been configured to provide the individual employee with access to the Library network. This access will enable you to communicate with others (within and outside of the Library), and share information and peripheral devices such as printers. The network connection is also a vital link to shared information resources and a range of desktop software tools.

3.2 Software Installation and Use
Software that has been licensed or provided by the Library may only be used on the Library's computer equipment, unless otherwise approved by the Employee’s Manager and Library Systems.

Library Systems will ensure that a computer will be available on which to test the software and assess the impact of any configuration changes. Library Systems is responsible for testing and installing approved software on the Library computer equipment. Any unregistered software is to be removed with the assistance of Library Systems.

Caution: The simple act of installing software on your computer will alter its configuration and may result in disruption to your network access.

Please contact the Helpdesk prior to acquiring any software so that Library Systems can evaluate the compatibility and system requirements of the software.

All software on Library computer equipment must be used in accordance with its license/copyright agreement and must adhere to its registration restrictions. For each software program installed on behalf of an employee's service unit, a complete registered program package will be retained by Library Systems.

It is a violation of the policy to install copies of home software (e.g. games, income tax programs) on Library computer equipment.

3.3 Hardware Installation and Use
Library Systems will arrange and coordinate all services, which relate to installation of new hardware and replacement and/or relocation of existing hardware and peripherals.

Library Systems may require up to five business days advance notice to install or move equipment. Please contact the Helpdesk to schedule moves.

It is a violation of this policy to install employee-owned hardware on Library computer equipment.

3.4 Monitoring
Utilities have been put in place to network activity and computer equipment. These will identify non-library applications, license infringements, and inappropriate file content such as games, pictures, music and animation files. Library Systems reserves the right to block, restrict or filter the usage of unregistered software and or hardware.

3.5 Back-up Procedures
Library Systems is responsible for backing-up all files/data stored on the Library network drives as well as application/database servers and e-mail mailboxes.

3.6 Piracy
Copying software (piracy) is theft and considered a criminal offence under Canadian Law.

It is the responsibility of the employee and management to ensure pirated software is not loaded on Library computer equipment.

3.7 Maintenance
It is the responsibility of each employee of the Library to maintain the data they are responsible for on the network. File maintenance and management should be performed on an on-going basis, subject to the *Records Management Policy*, to eliminate unnecessary information on the servers.

Section 4 – Policy for the Use of Library Applications

Please ensure that you also review Sections 1 and 2 which also contain guidelines on Applications.

4.1 Introduction

Applications and Library databases are used to store, modify, track and report on information that is typically considered valuable to one or more major service units.

4.2 Request for Access

Should access to an application be required, a request for access must be approved by the employee's Manager.

4.3 Access

Each employee's security access is based on the employee's individual leve1 of authority to access or modify information. For auditing purposes, employee ID's and passwords are recorded by the application/system. ID's or passwords are not to be shared. If and individual shares his/her ID they could be liable for all transactions and will be dealt with as having violated the Information Technology Use Policy.

4.4. Restore and Back-up Restores

Library Systems provides back-up and restore services for all Library applications. Requests to restore information must be made by the Manager of the service unit.

Section 5 – Email Policy

Please ensure that you also review Sections 1 and 2 which also contain guidelines on e-mail use.

5.1 Introduction

The primary purpose of the Library's e-mail system is for Library business communication. An email is a Library business record the same way that a memorandum or letter is a business record. Therefore, e-mail business communication should be treated in the same manner as any other business correspondence, i.e. communication that is inappropriate under the Library's logo, is inappropriate in e-mail.

5.2 Viruses

E-mails from known or unknown sources may contain viruses, which can cause repercussions on the entire Library infrastructure and system resources. Employees should not open e-mails containing unexpected attachments. It is the responsibility of all employees to exercise caution when receiving any e-mail containing attachments. E-mails from known or unknown sources may contain viruses, which can cause repercussions on the entire Library infrastructure and system resources.

5.3 Privacy and Confidentiality

Employees should be aware that their messages may not be completely private and are cautioned as to the confidential nature of their e-mail messages:

- the Library may be required to access the information,

- a recipient may have authorized another person(s) to read his or her e-mail,
- the message can be forwarded to another party or printed.

5.4 Personal Information
The decision to send personal information through e-mail should be considered when making this information available to other staff. An e-mail containing personal information should be sent only to staff members who need it in the performance of their duties. The e-mail should not be copied to an individual for information purposes only. In no circumstances should e-mail containing personal information be forwarded or copied to individuals outside the Library unless the individual to whom the information relates, consents to the disclosure and is copied on the e- mail.

5.5 Monitoring
In order to help ensure the security and stability of the Library e-mail utilities have been installed to scan all e-mail transactions.

These utilities will scan all e-mails including attachments and have the capability to check for specific words as well as file types and potential viruses. Library Systems reserves the right to block, restrict or filter the email transactions to maintain the overall security of the network and act upon inappropriate email content (5.2)

5.6 Inappropriate E-mail Content
While it is not possible to provide an all-inclusive list of inappropriate e-mail communication, certain types of information should not be communicated via e-mail. These include, but are not limited to:

- information which is, or may be, offensive or disruptive (such as communication that could constitute workplace harassment - refer to the *Ontario Human Rights Code* and the *Internal Workplace Harassment Prevention Policy),*
- information which is derogatory to any individual or group, or which is defamatory or threatening in nature,
- information which misrepresents the view of the Library,
- information which is disseminated for a purpose which is illegal, or for a purpose which contravenes the Library's policies or which is not in the interest of the Library, including confidential or sensitive business information,
- information for the purpose of promoting or advertising an employee's personal business, and
- information which includes chain letters, greeting cards, jokes, inspirational messages, sporting pools, junk mail, bulk mail, recipes, animation and videoclips.

5.7 Maintenance
It is the responsibility of each employee to regularly delete or archive messages that are no longer required. Due to storage capacity limits on the network, each employee is allocated a certain amount of storage space. If the limit is exceeded, you will be notified via a System Administrator message to delete or archive some of the stored e- mail.

These limits are enforced in order to protect the integrity of the e-mail system.

Section 6 – Internet Policy

Please ensure that you also review Sections 1 and 2 which also contain guidelines on Internet use.

6.1 Introduction

The Internet enables employees to gather information relevant to the Library and its businesses from external sources, and to provide Library information to Library users. The Internet also enables employees to research relevant topics and to obtain and prepare useful business information. It is the responsibility of the employee's Manager to determine the need for employee access to the Internet.

6.2 Privacy

No information should be viewed, copied or saved which is not relevant to Library business. Information which would not be distributed to members of the public (e.g. draft reports, confidential information, *Municipal Freedom of Information and Protection of Privacy Act* protected information) may not be posted on the Internet. No information should be distributed on the Internet which would not be appropriate for distribution under the Library's letterhead or logo.

6.3 Inappropriate Material

No employee shall access, upload or post inappropriate material, send or receive inappropriate material through the Internet e-mail or download inappropriate material through the Internet.

6.4 Monitoring

Utilities have been put in place to monitor Internet usage. The software provides detailed reports on sites visited and time spent on the Internet. Library Systems reserves the right to block, restrict or filter the usage of inappropriate material, internet email, purchases and downloading of files.

6.5 Internet E-mail

E-mail that is sent or received through the Internet is subject to the same guidelines as Internal e-mail. Please refer to Section 5 - E-mail Guidelines, for more detailed information.

6.6 Purchasing Via the Internet

Purchasing via the Internet will be in accordance with the *Purchasing Policy*.

6.7 Downloading of Files

Employees should be mindful of the costs, bandwidth and space requirements when downloading information from the Internet, as information is easily accessible through the Internet it does not necessarily need to be stored on the Library's network drives.

If necessary, business related information may be downloaded from the Internet. Any files that have been downloaded must be scanned for viruses.

Employees must respect copyright restrictions when downloading information from the Internet.

Section 7 - Administration

It is the responsibility of Library Systems to monitor and report infractions. Library Systems is also responsible for reviewing and updating the Information Technology Use Policy and Supporting Procedures Documents on an annual basis.

This policy will be reviewed annually and is available in alternative format upon request.