Adoption Date:	January 2018
Revision Date:	
Reference #:	SMT - 04
Category:	Operations

Employee Technology and Internet Use

1. PURPOSE

This policy has been established to provide governance and awareness for the acceptable use of technology standards and processes, network resources and the overall Business-Technologies and Infrastructure at the Brampton Library by library employees, contractors, volunteers, or third-parties vendors.

2. SCOPE

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

3. GENERAL ACCEPTABLE USE

Every user needs to exercise good judgment on the appropriate use of the business technologies and infrastructure at the Library in accordance with legislation and corporate policies.

The utilization of the technology and technology services shall be reserved for conducting Library business and shall not be used for any unlawful or prohibited purposes, whether explicitly identified herein or reasonably deemed unlawful or prohibited.

Technology and technology services are made available to library staff, Contractors or volunteers for business purposes. Although occasional personal use might occur, usage should not be excessive, impact work productivity or interfere with work performance. Users are encouraged to ask their direct supervisor or the Library Help Desk if they have any question regarding the appropriate use.

For security, compliance, and maintenance purposes, authorized staff may monitor and audit equipment, systems, and electronic communication. Unauthorized software, hardware or devices that may interfere with this corporate policy or deemed malicious, may be disabled, disconnected and/or confiscated without notice.

Exceptions to this policy must be approved by the CEO of the Library or authorized delegates. An "Exception to Policy Request" must include valid business justification and documented approvals from the requestor's supervisor.

4. ACCESS TO TECHNOLOGY

4.1. Users accessing technology or technology services (within the office or remotely) must adhere to the Library Governing Principles and the following provisions:

4.1.1. Be responsible for the security of account(s) under their control and to keep their password secured at all times

4.1.2. Shall not share such account(s) or password information with anyone, including other employees, third-party, family, or friends

4.1.3. Shall not provide access to another individual, either deliberately or through failure to secure such access

4.1.4. Ensure that Library information assets remain within the control of the Library at all times. The storage of Library-owned information on unauthorized devices is prohibited.

4.1.5. Reasonable use of and access to personal devices, accessories and digital information are not restricted to Library owned or leased end-user computing devices such as (laptop, desktop, tablet or smartphone). The storage and use of personal multimedia, files and/or tools on Library's file shares or shared data repositories are prohibited.

4.2. Be responsible for the security and appropriate use of technology and technology services under their control; and shall not be used for any of the following:

4.2.1. Circumventing security, user's login credentials (e.g. user ID and password) or causing a security breach

4.2.2. Accessing accounts without proper authorization

4.2.3. Downloading or introducing inappropriate content or software with intentions to probe, scan, cause harm or loss or damage

4.3. Causing a disruption of service to the Library, by performing non-business activities including but not limited to, gaming, audio/video downloading or playback, storing non Library data, moving or disconnecting shared devices under the control of the Library; and violating copyright laws, and/or contractual obligations including, but not limited to, illegally duplicating or transmitting copyrighted or restricted software and content such as data, pictures, music, video, etc.

4.4. Users who manage and use generic system account(s) to administer business processes and controls are accountable at all times to safeguard the use of such account(s); refrain from impersonating or misuse of these account(s) to hide their identity; and/or share these account(s) with others for same.

4.5. All users must not engage in any other activity not explicitly stated herein but reasonably deemed to be unlawful or prohibited.

5. PROTECTION OF PHYSICAL TECHNOLOGY ASSETS

5.1. Users are responsible:

5.1.1. For the physical technology assets under their control including, but not limited to, computing devices and systems, telephones, mobile devices, technology peripherals and accessories (e.g. printers, scanners, keyboard/mouse, speakers, software, etc.)

5.1.2. To secure and ensure the protection of assigned Library physical technology assets; and promptly report to the Library Help Desk any theft of, or damage to, the assigned physical technology assets

6. ELECTRONIC DATA AND INTELLECTUAL PROPERTY

All information assets shall remain the intellectual property of the Library and should be used in accordance with corporate policies, relevant licenses, contractual terms and conditions.

Users shall take all reasonable precautions to protect the information assets of the Library. Information assets that are generally made available to the public, service providers or third-party working with, or on behalf of the Library, must be appropriately protected, either through non-disclosure, contractual agreement, or appropriate disclaimer indemnifying the Library.

Distribution of these information assets are subject to legislation, Library's by-laws, policies and/or provisions outlined in contractual agreements.

7. ENFORCEMENT AND MONITORING CONTROLS

The Library typically monitors and/or logs access and usage activity of the technology and technology services to ensure compliance with this Policy and MFIPPA.

The Library reserves its rights to revoke or block access and/or usage of any technology or technology services or resources if deemed necessary, with or without notice.

8. ACTIONS FOR NON COMPLIANCE

Users in violation of this Policy will be reported to the appropriate level of management and/or the CEO.

Violators of this policy may be subject to disciplinary actions up to, and including, termination of employment or contract.

Violators for unlawful purposes may be subject to criminal prosecution, civil actions or both.