Last Updated:	Reviewed:	Point of Contact:
February 2018	Annually	Kathy Williams, Director of Public Service
Policy Number: P04		**Pages: 3**

Public Internet Use Policy

Policy Statement

The Pickering Public Library recognizes the internet as fundamental in fulfilling its mission of enriching the personal, civic and corporate lives of our community through access to ideas and information.

Policy Principles

1. In providing public access to the internet, the Library recognizes the shortcomings and dangers of an unregulated, worldwide environment. Internet content may be reliable and authoritative, or controversial and offensive: the client must assess the validity of all information found.

2. Children's access to and use of the internet is the responsibility of parents or guardians**.**

3. In order to maintain an environment that is safe and welcoming for all members of the community, the Library uses a commercial internet filter to block explicit sexual content. The Library recognizes that filtering software is imperfect; it does allow some inappropriate content to pass through and can block appropriate sites from view. Library staff have the ability to unblock content if necessary.

4. The Library reserves the right to modify or restrict access to the Internet, in full or in part, in order to carry out the service priorities of the organization.

5. Public Internet Use

a) The Library assumes no responsibility for any damages or expenses incurred as a result of the use of the internet at the Library. The Library will not be responsible for any personal information (e.g. credit card numbers or PIN numbers) that is compromised.

b) Certain copying or distribution of material found on the internet may infringe on the copyright laws of Canada; the library accepts no responsibility for such infringements.

c) While using the Library's Internet connection, clients may not:
   - Make any attempt to damage or disrupt service on the Library's computer networks.
   - Run network sniffer software, operate wireless access points or any utilize other means to intentionally intercept other users' data.
   - Submit, publish, or display any defamatory, abusive, obscene, threatening or illegal material.
   - Canvas, sell, promote, distribute or display unsolicited material (e.g. SPAM email).
   - Use Library computer networks or workstations for any illegal or criminal purpose.
   - Violate copyright laws or software licensing agreements in their use of Library computer networks.

d) Library clients must be respectful of the online experience of other clients using the network. Clients are asked to ensure that their activity does not impose an unusually large burden on the Library's network. The library may limit bandwidth capabilities of users who abuse the service.

e) If a website is blocked by the Library's filtering software that a client feels should be allowed, the client should notify staff. A staff member will review the request and allow access if appropriate.

6. **Public Internet Use on Library Computers**

a) Library clients must not use library workstations in a manner that results in damage or other harm. Clients must not install, delete or modify software on Library workstations.

b) Library clients must be aware that the Library's workstations are located in a public environment, which is shared by users of all ages and sensibilities. The Library is unable to ensure client privacy at our workstations and Library clients must be responsible for the sites that they select. Sites that may offend or disturb others should be closed immediately.

c) Library clients must respect the privacy of others using library workstations.

d) A Library card is not required to log on to the public workstations and there is no set time limit. The Library reserves the right to request a library card if internet abuse is suspected.

7. Public Internet Use of Wireless Network

a) Clients use the Library's wireless network at their own risk. The wireless network is not secure, as it is not encrypted. Unless additional precautions are taken, any

information you send using a wireless device could potentially be intercepted by a third party.

b) Clients are expected to use headphones when playing sound files to be considerate of clients nearby.

c) The Library is not responsible for laptops or other devices left unattended.

d) Clients are not permitted to tamper with any equipment belonging to the Library (e.g. unplugging library machines in order to use outlets or network cables).

e) The Library will not be responsible for any damage caused to client hardware or software due to power surges, security issues, hacking, or viruses. Anti-virus and security protection are the responsibility of the client.

f) The Library recommends that all users take measures to secure their wireless devices and Internet communications by equipping them with the following items:
   - Functional, up-to-date antivirus software.
   - The latest service packs and security patches for their computer's operating system and software packages.
   - Personal firewall software.

   The Library does not provide any of the above-referenced items and cannot guarantee or otherwise be responsible for their effectiveness. It is the responsibility of the client to secure their devices and internet communications.

Possible consequences of violating any of the above rules include expulsion, loss of library privileges, and prosecution.

For further information please contact Kathy Williams at kathyw@picnet.org or 905-831-6265 extension 6251.

Alternate formats available upon request. Please talk to Library staff.