REPORT TO THE LIBRARY BOARD  
Meeting date: November 26, 2009

<table>
<thead>
<tr>
<th>Session:</th>
<th>Public Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject:</td>
<td>Internet Service Policy: Annual Review</td>
</tr>
<tr>
<td>Prepared By:</td>
<td>Senior Team</td>
</tr>
<tr>
<td>Presented By:</td>
<td>Susanna Hubbard Krimmer</td>
</tr>
<tr>
<td>Purpose of Report:</td>
<td>For Decision: Approval ☑</td>
</tr>
</tbody>
</table>

**Recommendation**

It is recommended that the London Public Library (LPL) Internet Service Policy, per Library Board motion LA 08/57 and as provided in Appendix 7 of this report, remain in effect and that no changes be made at this time. It is also recommended that:

- Administration continue to monitor the progress of:
  - Ontario Provincial Parliament, Bill 202, *Education Statute Law Amendment Act (Electronic Sexual Material)*, 2009; and
  - House of Commons of Canada, Bill C-58, *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet Service* and Bill C-209, *An act to prevent the use of the Internet to distribute pornographic material involving children*;
- Administration update the Library Board on matters related to the policy, as required, and
- The Library Board conducts its annual review of the policy in November 2010 per the current policy.

**Purpose**

The Library Board is undertaking its annual review of the LPL *Internet Service Policy*. The purpose of this report is to provide information to assist in that process and specifically to:

- Report on the implementation of the *Internet Service Action Plan* developed following adoption of the *Internet Service Policy* in November 2008;
- Provide a monitoring and review of the application of the *Internet Service Policy*;
- Identify supporting policies that address behavioural issues related to the public’s use of Internet services; and
- Recommend any changes to the *Internet Service Policy*. 
Issue / Opportunity

Libraries and information services provide access to information, ideas and works of imagination in any medium and regardless of frontiers. They serve as gateways to knowledge, thought and culture, offering essential support for independent decision making, cultural development, research and lifelong learning by both individuals and groups.

From LPL’s point of view, the Internet is the ideal vehicle to:

- Enhance public access to information and expressions of creativity and thought;
- Expand the library’s collection of information resources;
- Provide users with the opportunity for remote dialogue with subject-matter experts and to engage with other people on an infinite variety of topics; and
- Enable collaborative research and study.

LPL’s Internet Service is consistent with its Vision, Mission, Value Promise and Service Excellence Model. LPL offers Internet access as part of its suite of services to the public in an effort to meet community needs in the areas of: Literacy, Learning, Culture, Leisure and Recreation, Information, and Community Meeting Place.

Any policy adopted by the LPL will be based on two fundamental principles: Providing the broadest Internet access possible to its patrons in a way that is in accord with the Canadian Charter of Rights and Freedoms and which includes due regard for the privacy of patrons who access the Internet.

In instances when exceptions to the above are necessary to protect others (i.e. minors) the restriction should be as minimally invasive as possible.

The challenge is to create balance between the rights of individuals to access a wide range of information resources with the rights of users and staff to work in a public environment.

Background & Review Summary

The current Internet Service Policy was adopted by the Library Board at its meeting of November 27, 2008 (L08/57). The LPL’s Internet Service Action Plan was also adopted along with the direction that the policy be reviewed annually or at such time within the annual framework as may be necessary.
Policy Development & Review

In developing its current policy, LPL considered:

- Philosophical context;
- Constitutional and legal context;
- Legal opinions, i.e. due diligence on Internet access in public libraries;
- Public policy context, e.g. policy statements of Canadian public libraries;
- Service best practices;
- Technology-based tools, e.g. filtering software; and
- Strategies for promotion of media awareness and safe surfing.

LPL has instituted a continual process of environmental scanning to ensure that we are current on all elements of the policy framework.

Legislative Environment

The legal framework within which the current Internet Service Policy was developed includes, for example: Canadian Charter of Rights and Freedoms, Canadian Human Rights Act, Copyright Act, Criminal Code of Canada, Telecommunications Act, Broadcasting Act, Film Classification Act, Public Libraries Act and City of London By-laws.

We are currently monitoring a provincial legislative bill which, if enacted, would impact the legislative environment and the LPL Internet Service Policy. A bill before the Ontario Provincial Parliament, Bill 202, Education Statute Law Amendment Act (Electronic Sexual Material), 2009 would amend both Education Act and Public Libraries Act. This bill would make it mandatory that “pornography” filtering systems be installed for all computers in schools and libraries in Ontario. On September 16, 2009, it passed first reading in the provincial legislature. The Bill was carried in second reading on October 1, 2009 and has been referred to the Standing Committee on Regulations and Private Bills.


The Federation of Ontario Public Libraries has voiced its concern to the government regarding implications to public library service.

As a result of the introduction of Bill 202, information packages were sent by London Public Library to local area Members of Provincial Parliament so that they were apprised of LPL’s policy and practices and how this shows public policy in action, i.e. how public library Internet service is offered in a practical setting.
Current Internet Service Policy

Highlights of the current Internet Service Policy include:

- Incorporation of guiding principles;
- Incorporation of library, user and staff responsibilities;
- Provision of broad access to content
- Access to content is limited only by the extent required for the protection of children and teens which will affect LPL filtering practice;
- A statement of consequences for inappropriate behaviour and/or unlawful activity; and
- A required annual review.

Consistent with the Internet Service Policy, LPL has in place:

- Privacy screens on monitors, privacy partitions;
- Complaints/Incident reporting process and procedures;
- Staffing training; and
- Web awareness tools and programming.

Users are responsible for:

- Following the Library's Charter of Use, Rules of Conduct and other policies related to conduct in library space;
- Respecting the rights of others when accessing Internet sites in library space;
- Respecting the privacy of other library patrons; and
- Determining the legality of any sites they access.

LPL provides a combination of unfiltered and filtered Internet access across the system and at each location:

- Computers specifically designated for use by children and/or teens, such as Homework Centre Computers, are filtered;
- Computers in spaces specifically designed for use by children and/or teens are filtered;
- Computers designated for specific functions, such as the Employment Resource Centre computers, are filtered; and
- All other computers, including wireless connections, are unfiltered.

Note: Exceptions occur in cases in which all other methods of due diligence regarding the reasonable protection of children/teens cannot be achieved.
**Overview of Computer and Internet Usage**

The following comparative statistics for 2007, 2008 and 2009 (projected) provide a context for Internet usage discussed in this report.

<table>
<thead>
<tr>
<th>Table 1: Comparative Annual Computer Usage Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Indicator</strong></td>
</tr>
<tr>
<td>Use of Internet workstations*</td>
</tr>
<tr>
<td>Wireless usage</td>
</tr>
<tr>
<td>Total computer workstation usage</td>
</tr>
</tbody>
</table>

*excluding OPAC’s (Online Public Access Catalogues)

**Report on LPL Internet Service Action Plan**

An *Internet Service Action Plan* was approved by the Library Board in November 2008 in order to implement changes in the public service areas and related functions required by the adoption of the *Internet Service Policy*. Elements of the *Action Plan* included staff training, the assessment and adjustment of the technical and physical environments, and external and internal communications.

See *Appendix 2: LPL Internet Service Action Plan*.

An Internet Service Implementation Team whose role it was to lead and oversee the implementation of the new policy and to make recommendations for future changes to policy or practice was established. Members included: Sarah Andrews, David Caloren, Nancy Collister, Rob Kearns, Susanna Hubbard Krimmer, Margaret Mitchell, Christina Nurse, Brian Rhoden, Arlene Thompson, Tom Travers, and Margaret Wilkinson.

The implementation of the *Internet Service Action Plan* was complete March 31, 2009. Customer Services & Branch Operations, IT, Communications, Facility Services and Human Resources Staff and Supervisors contributed to the implementation of the plan. A detailed report of activities is contained in *Appendix 3: Internet Service Action Plan: Implementation*.

**Physical Environment**

The assessment and adjustment of the physical environment, done in conjunction with changes to the technical environment, was the most time consuming and labour intensive component of the *Action Plan*. At the same time, this piece was essential to
the successful achievement of the guiding principles of access and service upon which the policy is based.


**Staff Training and Support**

Staff training and support was identified an essential component of the implementation plan and the Internet Service Policy Implementation Team developed the following training goals for staff:

- To review and ensure awareness of the Internet Service Policy;
- To understand the rights and obligations of users under the Policy; and
- To understand the processes and appropriate actions in the event the Policy is contravened by a user.

An e-learning module, procedure document and job aid were developed and distributed with all public service staff participating in the training. In order that employees new to the organization are aware of the Internet Service Policy, a component has been added to the corporate orientation program for new staff.


**Monitoring and Review of Policy Implementation**

Since the implementation of the Action Plan, in March 2009, we have monitored and reviewed the effect of the Internet Service Policy/Action Plan on daily services and operations by:

- Responding to incidents as they arise, documenting and tracking incidents using incident management process/forms, and following up with appropriate actions;
- Tracking of and responding to public/staff comments and feedback;
- Reviewing filtering software reports; and
- Reviewing on an ongoing basis furniture and equipment, e.g. privacy screens for monitors, in response to issues and concerns raised by the public and staff.

**Incident Reports Regarding the Viewing of Objectionable Content**

Incident reports are prepared by staff or security when infractions of Library policies have occurred or a patron has raised a concern about activity in the Library for which Library staff and/or security staff has been required to take some kind of action.

Appendix 4 contains a table of all incident reports filed relating to complaints from the public about viewing of objectionable content for 2008 and 2009 (to mid-November). This time frame was chosen to show the impact of both the current and previous policy. The table includes date, description, location and staff follow-up.

In 2008, 11 incident reports were filed, relating to patron concerns about the viewing of objectionable content at computer workstations. In 2009, to date 24 incident reports have been filed. The number of incidents in 2009 concerning the viewing of objectionable content is higher than in 2008. Several things may account for this difference. First, the ratio of unfiltered to filtered workstations changed with more workstations being unfiltered since March 2009. Secondly, staff procedures have clarified reporting requirements for issues arising. Finally, heightened awareness, due to the arrest made in August 2009, related to the alleged viewing of child pornography, may have encouraged more patrons to voice concerns.

Table 2 below summarizes occurrences of incident reports.

<table>
<thead>
<tr>
<th>Type</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objectionable Internet content</td>
<td>11</td>
<td>24</td>
</tr>
<tr>
<td>Total Incidents</td>
<td>670</td>
<td>380</td>
</tr>
</tbody>
</table>

The total number of incidents decreased significantly in 2009. This is primarily due to the introduction of the Pharos system for patron authentication which was installed on public Internet computers, system wide, by June 2008. The Pharos system requires that the patron be a user in good standing with a valid library card to access computers. The system prevents misuse of access privileges which prior to the Pharos implementation, were a major source of patron incidents. After June 2008, there was a significant reduction in such incidents.

Table 3 below compares the total number or incidents related to the viewing of objectionable content on the Internet compared to total Internet usage, measured by the number of log-ons, for the same time period.

<table>
<thead>
<tr>
<th></th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Incidents</td>
<td>11</td>
<td>24</td>
</tr>
<tr>
<td>Total Internet Usage (log-ons)</td>
<td>480,228</td>
<td>493,000</td>
</tr>
<tr>
<td>Percentage</td>
<td>.003 %</td>
<td>.005 %</td>
</tr>
</tbody>
</table>
Of those reported incidents of viewing of objectionable content, most occurred at the Central Library.

The Library recognizes that, while the number of incidents is proportionately small compared with the total number of Internet uses, for individual users an incident of exposure may be disturbing on a personal basis. Therefore, all information and feedback gathered as part of the incident reporting process is carefully reviewed to determine if there is anything we can do better in terms of technological and physical solutions to prevent unintentional exposure to content.

Public Feedback

LPL also receives feedback from library users and other members of the public about Library services either in person, through the “How Did We Do Today?” Form, via e-mail, on the telephone, etc. The Library records all of this feedback in order to assist in gauging public response to services and taking appropriate steps on issues that may arise.

Since August 2009, when the alleged child pornography incident occurred at the Central Library and the incident and subsequent arrest were publicly reported, Library Administration has received correspondence from 12 individuals with regards to LPL’s policy and practices. Comments relate to the viewing of “pornography” on computers in the Library and/or filtering.

See Appendix 5: Public Feedback Since November 2008 Internet Service Policy. Note: Two of the emails are input from individuals who reside outside of London/Middlesex County, i.e. Nova Scotia and Sudbury.] The correspondence listed in the appendix, along with the media coverage, was previously received by the Library Board in September and October, 2009.

Net Alerts (URL Inquiries)

LPL has implemented a “net alert” option, whereby users of filtered workstations, who encounter a blocked site that they believe has been incorrectly categorized as “pornography” (and therefore filtered), may send an alert to Netsweeper. Netsweeper's process is to then review the categorization of the site.

Access to URLs categorized as Pornography

In the 2007 November report to the Library Board on the Internet and Computer Use Policy, graphs were presented which provided a view of the access to URLs categorized as “pornography” during the month of October 2007. The study compared the number of URLs accessed in selected categories and provided information on system-wide activity.
Netsweeper data was reviewed for Sept 2009. While the data cannot be compared directly as the mix of unfiltered versus filtered workstations has changed substantially from 2007 to 2009, the charts do provide a general comparison regarding the proportion of access to URLs categorized as “pornography” compared to other uses of the Internet. In 2009, System-wide access to sites categorized as “pornography” ranked 11th.


A further analysis of overall URL access is presented in Table 4 below. The analysis is based on the study parameters of 2007, as presented in Appendix 6.

| Table 4: Comparison of Increase in Traffic on Unfiltered Workstations, Oct 2007 and Sept 2009 (Using 2007 selected categories related to information and social networking) |
|--------------------------------------------------|---------|--------|
| System-Wide                                      | 2007    | 2009   |
| Unfiltered Total URLs                            | 562,215 | 2,476,213 |
| Unfiltered URLs categorized as Pornography       | 35,114  | 82,715 |
| % of URLs categorized as Pornography             | 6.2%    | 3.3%   |

While access to the total number of URLs has increased exponentially on unfiltered workstations, access to URLs categorized as pornography has not experienced the same level of increase.

It should be noted that these are snapshot studies and cannot be used to draw conclusions about specific aspects of Internet usage. Nevertheless the overall general indication is that access to URLs, categorized as “pornography”, is not a comparatively high percentage of Internet usage system-wide.

**Ongoing Review of Furniture and Equipment Placement**

Since March 2009, LPL has continually reviewed furniture and equipment layout to help minimize unintentional exposure to content being viewed on computer screens and to support user privacy. As necessary, changes are made to the placement of computer workstations. As well, LPL has tested a variety of new privacy screens and “hoods” for monitors. Products did not noticeably reduce visibility of content on computer screens for walk-by traffic as compared with products LPL has in use. Staff continue to seek improved solutions.
**Communications**

A Communications Strategy to inform community stakeholders, including partners, of the changes to the policy was developed and implemented as part of the *Internet Service Action Plan*. The key elements of the plan were to:

- Create awareness and understanding about LPL's valuable Internet Service and its benefits to the user;
- Convey information about the LPL Internet Service Policy and its context;
- Provide information about any changes that will affect users and staff;
- Engage staff and community partner participation in the creation and implementation of new practices to ensure that the service is relevant, accessible and high quality and effective and efficient from an internal perspective;
- Encourage user media awareness and Internet safety;
- Ensure staff knowledge, capabilities, empowerment and confidence in providing information, answering questions and responding to queries, concerns and complaints;
- Provide opportunities for public improvement of the LPL Internet service.

An action following the setting of the new policy was a liaison meeting of the LPL CEO with London Police Chief Murray Faulkner and Detective Dale Howe (Cybercrime Unit) to discuss the policy changes and possible implications. LPL Staff have worked with Detective Howe and his team for a number of years and an outcome of this meeting was joint action undertaken by Detective Howe and LPL staff to confirm and enhance communications protocols when there is a perceived/alleged contravention of the law, such as the Criminal Code, by a library user. The effectiveness of LPL-LPS communications was demonstrated by the fact that both parties acted expeditiously and effectively in the child pornography incident leading to the laying of charges by the police.

The communications strategy is being used on an ongoing basis, for example:

LPL has continued to promote the use of the Internet as a valuable information resource and communications conduit. For example, given the over 3 million hits on the LPL website, we continue to use this as a venue to link people with current information on topical subjects, such as the H1N1 flu information. Most recently we worked with the Middlesex County Library to support the United Way in reaching out to Londoners via the Internet to seek input on issues facing the community (See correspondence in Board meeting package from Andrew Lockie, CEO United Way of London & Middlesex).

LPL has continued to undertake web awareness initiatives. In April 2009, as part of London Technology Week, in partnership with the London Police Cyber Crime Unit, TD Bank Financial Group and TechAlliance, the Library hosted a “Parent Internet-Safety Seminar”. London Technology Week is a community celebration of London's technology community and its contribution to our city’s economy, well-being and quality of life. This year, TD Bank Financial Group and TechAlliance decided to pursue the
idea of offering a seminar for parents and caregivers on Internet Safety. They engaged the London Public Library and the London Police Services (Cyber Crimes Unit) who agreed to lend their support to the initiative.

LPL’s *Internet Service Policy* and practices are being cited as a best practice for public libraries. LPL staff have been approached by and provided several libraries with information and advice in the area of web awareness and media literacy.

**Alignment of Internet Service Policy with other LPL Policies**

London Public Library endeavours to provide a welcoming and safe environment for the enjoyment of the public and staff so that all persons may enjoy the benefits of the Library. The *LPL Charter of Library Use* and all related policies require that individuals using Library services and resources are expected to act with respect and consideration for others and for Library property. Library Staff are entrusted with the obligation to ensure that policies for Library use are followed and will apply these policies in a fair, dignified and positive manner for the benefit of all. Any person violating Library rules risks suspension of Library privileges, exclusion from the Library, cost-recovery damages and prosecution. The policies empower and require staff to respond to inappropriate behaviours that may occur when people are using any of the services provided by the Library.

Each of the *Charter of Library Use* policies, below, applies to people using LPL’s Internet Service. The clarity around this in our staff procedures and training has resulted in more timely, effective and appropriate follow up on issues. We have also endeavoured to communicate publicly that there are consequences for inappropriate behaviours (including those by someone using the Internet in a library location) to underscore that LPL is working hard to create a welcoming and safe environment for everyone.

*Rules of Conduct*

The purpose of this policy is to address expectations and issues regarding behavior of patrons in the Library. It sets out expectations regarding mutual respect, safety of children, respect for library property, and accessing and using intellectual content and establishes consequences for violation of the rules including loss of library privileges, banning and prosecution.

Members of the public and staff are expected to act with respect and consideration for others. Behaviour that is disruptive, intrusive, lewd, abusive, harassing or threatening to Library users or staff is not permitted. Abusive or obscene language is not permitted.

*Unattended Children Policy*

The purpose of this policy is to address the issue of children left unattended in the Library. An unattended child is a child left without visible supervision within the library.
This policy applies to all children, under the age of 12, in all locations across the London Public Library System. Parents, guardians or caregivers are responsible for providing supervision and care of their children while a child is on the premises of London Public Library. It is the responsibility of the parent or caregiver to monitor both the whereabouts and behaviour of their children while on Library premises. Library staff cannot care for nor take responsibility for children left unattended at the Library.

**Computer Use Policy**

This policy was updated in 2009 and pertains to the use of computer hardware, software, networks, vendor software licenses, and other related entities. The purpose of this policy is to outline: the Library’s responsibilities in providing computers for public use; the user’s responsibilities in using library computer hardware, software and related equipment; staff responsibilities in response to situations; and consequences of inappropriate behaviour and/or illegal activity by users.

**Summary and Recommendation**

In November 2008, the Library Board instituted an *LPL Internet Service Policy* based on the principles of

- Providing the broadest Internet access possible to its patrons in a way that is in accordance with the Charter, which includes due regard for the privacy of patrons who access the Internet through unfiltered terminals; and
- In instances when exceptions to the above general principle are necessary to protect others (i.e. minors) the restriction should be as minimally invasive as possible.

In order to comply with these principles, the Board policy includes a mix of computers with filtered and unfiltered Internet access. To achieve this, Staff reviewed and adjusted computer placement and installed privacy equipment in all locations putting in place measures to minimize the risk of inadvertent exposure to content being viewed by computer users, to protect the privacy of individuals and to provide good library customer services. Staff received training in the policies and procedures, including procedures for dealing with complaints/concerns.

The Ontario Provincial Parliament, Bill 202, *Education Statute Law Amendment Act (Electronic Sexual Material)*, 2009, if passed, would have significant impact on the LPL Internet Service Policy. Given that the Bill has progressed to standing committee review after second reading, it would be advisable to await the outcome of the legislative process before considering any revisions to the current policy. Administration will continue to monitor this situation closely and report back to the Library Board as required.
Bill 202, Education Statute Law Amendment Act (Electronic Sexual Material), 2009
Martiniuk, Gerry

Current Status: Ordered referred to the Standing Committee on Regulations and Private Bills

Status

<table>
<thead>
<tr>
<th>Date</th>
<th>Bill Stage</th>
<th>Activity</th>
<th>Committee</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 01, 2009</td>
<td></td>
<td>Ordered referred to Standing Committee</td>
<td>Standing Committee on Regulations and Private Bills</td>
</tr>
<tr>
<td>October 01, 2009</td>
<td>Second Reading</td>
<td>Carried</td>
<td></td>
</tr>
<tr>
<td>October 01, 2009</td>
<td>Second Reading</td>
<td>Debate</td>
<td></td>
</tr>
<tr>
<td>September 16, 2009</td>
<td>First Reading</td>
<td>Carried</td>
<td></td>
</tr>
</tbody>
</table>

Bill 202

An Act to protect our children from pornography

Mr. Martiniuk

Private Member’s Bill

1st Reading  September 16, 2009
2nd Reading
3rd Reading
Royal Assent
EXPLANATORY NOTE

Education Act

The Bill amends the Education Act to require every school board to ensure that every school of the board has in place technology measures on all of the school's computers to which a person under the age of 18 years has access. The technology measures must do the following:

1. They must block access on the Internet to any material, including written material, pictures and recordings, that is obscene or sexually explicit or that constitutes child pornography.

2. They must block access to any form of electronic communication, including electronic mail and chat rooms, if the communication could reasonably be expected to contain any material, including written material, pictures and recordings, that is obscene or sexually explicit or that constitutes child pornography.

3. They must block access to any site on the Internet or to any form of electronic communication, including electronic mail and chat rooms, if the school has not authorized users of the computers to access the site or the communication or if the site or the communication could reasonably be expected to contain material that includes personal information about a person under the age of 18 years.

A school is required to have a policy on who are authorized to use its computers to which a person under the age of 18 years has access and to monitor the use that persons under the age of 18 years make of those computers.

Public Libraries Act

The Bill amends the Public Libraries Act to make amendments that are similar to those that the Bill makes to the Education Act, except that the duties of a school board are those of a board with respect to every library under its jurisdiction and the duties of a school are those of a public library.

Loi sur l'éducation

Le projet de loi modifie la Loi sur l'éducation de façon à obliger les conseils scolaires à veiller à ce que chacune de leurs écoles dote tous ses ordinateurs auxquels ont accès des personnes de moins de 18 ans de moyens technologiques qui font ce qui suit :

1. Bloquer l'accès sur Internet à des documents — écrits, images et enregistrements — qui sont obscènes ou sexuellement explicites ou qui constituent de la pornographie juvénile.

2. Bloquer l'accès à toute forme de communication électronique, notamment le courrier électronique et les clavardoirs, dont il serait raisonnable de s'attendre à ce qu'elle contienne des documents — écrits, images et enregistrements — qui sont obscènes ou sexuellement explicites ou qui constituent de la pornographie juvénile.

3. Bloquer l'accès à tout site Internet ou à toute forme de communication électronique, notamment le courrier électronique et les clavardoirs, auquel l'école n'a pas autorisé les utilisateurs des ordinateurs à avoir accès ou dont il serait raisonnable de s'attendre à ce qu'il contienne des documents qui figurent des renseignements personnels concernant une personne de moins de 18 ans.

Les écoles doivent également adopter une politique permettant de préciser qui est autorisé à utiliser ses ordinateurs auxquels ont accès des personnes de moins de 18 ans et de surveiller l'usage que celles-ci en font.

Loi sur les bibliothèques publiques

Le projet de loi modifie la Loi sur les bibliothèques publiques pour y apporter des modifications semblables à celles qu’il apporte à la Loi sur l’éducation, sauf que les obligations d’un conseil scolaire sont celles d’un conseil à l’égard des bibliothèques relevant de sa compétence et les obligations des écoles sont celles des bibliothèques publiques.
An Act to protect our children from pornography

Note: This Act amends or repeals more than one Act. For the legislative history of these Acts, see the Table of Consolidated Public Statutes – Detailed Legislative History at www.e-Laws.gov.on.ca.

Her Majesty, by and with the advice and consent of the Legislative Assembly of the Province of Ontario, enacts as follows:

EDUCATION ACT

1. Section 230 of the Education Act is amended by striking out “or” at the end of clause (b), by adding “or” at the end of clause (c) and by adding the following clause:

(d) contravenes section 321, 322 or 323.

2. The Act is amended by adding the following Part:

PART XIII.2
PROHIBITING ACCESS TO ELECTRONIC FORMS OF SEXUAL MATERIAL

Blocking access to sexual material

321. (1) In this section,

“sexually explicit material” means material of which a principal feature or characteristic is the nudity or partial nudity of any person and that is designed to appeal to erotic or sexual appetites or inclinations.

Same

(2) A board shall ensure that every school of the board has in place technology measures on all of the school’s computers to which a minor may have access that,

(a) block access on the Internet to any material, including written material, pictures and recordings, that is obscene within the meaning of subsection 163 (8) of the Criminal Code (Canada) or sexually explicit or that constitutes child pornography within the meaning of section 163.1 of the Criminal Code (Canada); and

(b) block access to any form of electronic communication, including electronic mail and chat rooms, if the communication could reasonably be expected to contain any material, including written material, pictures and recordings, that is obscene within the
Monitoring electronic access by minors

322. (1) A board shall ensure that every school of the board has in place technology measures on all of the school’s computers to which a minor may have access that block access to any site on the Internet or to any form of electronic communication, including electronic mail and chat rooms, if:

(a) the school has not authorized users of the computers to access the site or the communication; or

(b) the site or the communication could reasonably be expected to contain material that includes personal information within the meaning of the Freedom of Information and Protection of Privacy Act about a minor.

Policy for authorized access

(2) A board shall ensure that,

(a) every school of the board has a policy to determine what minors or class of minors are authorized to use the school’s computers to access what sites on the Internet and what forms of electronic communication, including electronic mail and chat rooms;

(b) the policy described in clause (a) meets the requirements, if any, prescribed by the regulations; and

(c) every school of the board publishes a notice setting out the policy described in clause (a) in conspicuous places in the school, as the school determines and the regulations require.

Monitoring electronic access by minors

323. A board shall ensure that every school of the board,

(a) monitors the use by minors of any or all of the school’s computers to access the Internet or any form of electronic communication, including electronic mail or chat rooms for the purpose of allowing the board to determine whether it has met its obligations under section 321 or 322; and

(b) has in place technology measures that permit the school to perform the monitoring described in clause (a).

Regulations

324. (1) The Minister may make regulations,

(a) specifying standards that technology measures must meet for a board to comply with its requirements in section 321, 322 or 323;

323. Le conseil veille à ce que chaque école ait doté tous ses ordinateurs auxquels peuvent avoir accès des personnes mineures des moyens technologiques qui bloquent l’accès à tout site Internet ou à toute forme de communication électronique, notamment le courrier électronique et les clavardoirs :

a) soit auquel l’école n’a pas autorisé les utilisateurs des ordinateurs à avoir accès ;

b) soit dont il serait raisonnable de s’attendre à ce qu’il contienne des documents où figurent des renseignements personnels au sens de la Loi sur l’accès à l’information et la protection de la vie privée concernant une personne mineure.

Politique concernant l’accès autorisé

(2) Le conseil veille à ce qui suit :

a) chacune de ses écoles adopte une politique permettant de préciser les personnes mineures ou catégories de personnes mineures qui sont autorisées à utiliser ses ordinateurs pour avoir accès à des sites Internet ou à des formes de communication électronique, notamment le courrier électronique et les clavardoirs, et les sites et formes de communication concernés ;

b) la politique visée à l’alinéa a) satisfait aux exigences éventuelles prescrites par les règlements ;

c) chacune de ses écoles publie un avis énonçant la politique visée à l’alinéa a) à des endroits bien en vue dans l’école, selon ce que décide l’école et ce qu’exigent les règlements.

Surveillance : accès électronique par les personnes mineures

323. Le conseil veille à ce que chaque de ses écoles :

a) d’une part, surveille l’usage que font les personnes mineures de ses ordinateurs pour avoir accès à Internet ou à toute forme de communication électronique, notamment le courrier électronique et les clavardoirs, de façon à permettre au conseil d’établir s’il a rempli les obligations que lui impose l’article 321 ou 322 ;

b) d’autre part, se dote des moyens technologiques qui lui permettent de procéder à la surveillance visée à l’alinéa a).

Règlements

324. (1) Le ministre peut, par règlement :

a) préciser les normes auxquelles doivent satisfaire des moyens technologiques pour que les conseils se conforment aux exigences de l’article 321, 322 ou 323 ;
(b) prescribing or specifying anything that this Part describes as being prescribed or required in the regulations.

General or specific application

(2) A regulation made under this section may be of general application or specific to any person, persons, thing or things or class or classes in its application.

Classes

(3) A class described in the regulations made under this section may be described according to any characteristic or combination of characteristics and may be described to include or exclude any specified member, whether or not with the same characteristics.

PUBLIC LIBRARIES ACT

3. Part III of the Public Libraries Act is amended by adding the following sections:

Blocking access to sexual material

38.1 (1) In this section,

"sexually explicit material" means material of which a principal feature or characteristic is the nudity or partial nudity of any person and that is designed to appeal to erotic or sexual appetites or inclinations.

Same

(2) A board shall ensure that every library under its jurisdiction has in place technology measures on all of the library’s computers to which a minor may have access that,

(a) block access on the Internet to any material, including written material, pictures and recordings, that is obscene within the meaning of subsection 163 (8) of the Criminal Code (Canada) or sexually explicit or that constitutes child pornography within the meaning of section 163.1 of the Criminal Code (Canada); and

(b) block access to any form of electronic communication, including electronic mail and chat rooms, if the communication could reasonably be expected to contain any material, including written material, pictures and recordings, that is obscene within the meaning of subsection 163 (8) of the Criminal Code (Canada) or sexually explicit or that constitutes child pornography within the meaning of section 163.1 of the Criminal Code (Canada).

Blocking access to unauthorized material

38.2 (1) A board shall ensure that every library under its jurisdiction has in place technology measures on all of the library’s computers to which a minor may have access that block access to any site on the Internet or to any form of electronic communication, including electronic mail and chat rooms, if,

b) prescrire ou préciser tout ce que la présente partie mentionne comme étant prescrit ou exigé dans les règlements.

Portée générale ou particulière

(2) Les règlements pris en application du présent article peuvent avoir une portée générale ou ne s’appliquer qu’à des personnes, objets ou catégories particuliers.

Catégories

(3) Une catégorie visée dans les règlements pris en application du présent article peut être décrite selon n’importe quelle caractéristique ou combinaison de caractéristiques, et peut être décrite comme une catégorie incluant ou excluant tout membre précisé, que celui-ci soit doté ou non des mêmes caractéristiques.

LOI SUR LES BIBLIOTHÈQUES PUBLIQUES

3. La partie III de la Loi sur les bibliothèques publiques est modifiée par adjonction des articles suivants:

Accès bloqué : documents à caractère sexuel

38.1 (1) La définition qui suit s’applique au présent article.

«documents sexuellement explicites» Documents dont une des caractéristiques principales est la nudité intégrale ou partielle d’une personne et qui sont conçus pour stimuler les appréciations ou les tendances sexuelles ou érotiques.

Idem

(2) Le conseil veille à ce que chaque bibliothèque relevant de sa compétence doté tous ses ordinateurs auxquels peuvent avoir accès des personnes mineures de moyens technologiques qui :

a) d’une part, bloquent l’accès sur Internet à des documents — écrits, images et enregistrements — qui sont obscènes, au sens du paragraphe 163 (8) du Code criminel (Canada), ou sexuellement explicites ou qui constituent de la pornographie juvénile, au sens de l’article 163.1 du Code criminel (Canada);

b) d’autre part, bloquent l’accès à toute forme de communication électronique, notamment le courrier électronique et les clavardoirs, dont il serait raisonnable de s’attendre à ce qu’elle contienne des documents — écrits, images et enregistrements — qui sont obscènes, au sens du paragraphe 163 (8) du Code criminel (Canada), ou sexuellement explicites ou qui constituent de la pornographie juvénile, au sens de l’article 163.1 du Code criminel (Canada).

Accès bloqué : documents non autorisés

38.2 (1) Le conseil veille à ce que chaque bibliothèque relevant de sa compétence ait doté tous ses ordinateurs auxquels peuvent avoir accès des personnes mineures des moyens technologiques qui bloquent l’accès à tout site Internet ou à toute forme de communication électronique, notamment le courrier électronique et les clavardoirs:
(a) the library has not authorized users of the computers to access the site or the communication; or
(b) the site or the communication could reasonably be expected to contain material that includes personal information within the meaning of the Freedom of Information and Protection of Privacy Act about a minor.

Policy for authorized access

(2) A board shall ensure that,
(a) every library under its jurisdiction has a policy to determine what minors or class of minors are authorized to use the library’s computers to access what sites on the Internet and what forms of electronic communication, including electronic mail and chat rooms;
(b) the policy described in clause (a) meets the prescribed requirements, if any; and
(c) every library under its jurisdiction publishes a notice setting out the policy described in clause (a) in conspicuous places in the library, as the library determines and the regulations require.

Monitoring electronic access by minors

38.3 A board shall ensure that every library under its jurisdiction,
(a) monitors the use by minors of any or all of the library’s computers to access the Internet or any form of electronic communication, including electronic mail or chat rooms for the purpose of allowing the board to determine whether it has met its obligations under section 38.1 or 38.2; and
(b) has in place technology measures that permit the library to perform the monitoring described in clause (a).

Minister’s regulations

38.4 (1) The Minister may make regulations,
(a) specifying standards that technology measures must meet for a board to comply with its requirements in section 38.1, 38.2 or 38.3;
(b) specifying anything that section 38.2 describes as being prescribed or required in the regulations.

General or specific application

(2) A regulation made under this section may be of general application or specific to any person, persons, thing or things or class or classes in its application.

Classes

(3) A class described in the regulations made under this section may be described according to any characteristic or combination of characteristics and may be described to include or exclude any specified member,

(a) soit auquel la bibliothèque n’a pas autorisé les utilisateurs des ordinateurs à avoir accès;
(b) soit dont il serait raisonnable de s’attendre à ce qu’il contienne des documents où figurent des renseignements personnels au sens de la Loi sur l’accès à l’information et la protection de la vie privée concernant une personne mineure.

Politique concernant l’accès autorisé

(2) Le conseil veille à ce qui suit :
(a) chaque bibliothèque relevant de sa compétence adopte une politique permettant de préciser les personnes mineures ou catégories de personnes mineures qui sont autorisées à utiliser ses ordinateurs pour avoir accès à des sites Internet ou à des formes de communication électronique, notamment le courrier électronique et les clavardoirs, et les sites et formes de communication concernés;
(b) la politique visée à l’alinéa a) satisfait aux exigences éventuelles prescrites par les règlements;
(c) chaque bibliothèque relevant de sa compétence publie un avis énonçant la politique visée à l’alinéa a) à des endroits bien en vue dans la bibliothèque, selon ce que décide la bibliothèque et ce qu’exigent les règlements.

Surveillance : accès électronique par les personnes mineures

38.3 Le conseil veille à ce que chaque bibliothèque relevant de sa compétence :
(a) d’une part, surveille l’usage que font les personnes mineures de ses ordinateurs pour avoir accès à Internet ou à toute forme de communication électronique, notamment le courrier électronique et les clavardoirs, de façon à permettre au conseil d’établir s’il a rempli les obligations que lui impose l’article 38.1 ou 38.2;
(b) d’autre part, se dote des moyens technologiques qui lui permettent de procéder à la surveillance visée à l’alinéa a).

Règlements du ministre

38.4 (1) Le ministre peut, par règlement :
(a) préciser les normes auxquelles doivent satisfaire des moyens technologiques pour que le conseil se conforme aux exigences de l’article 38.1, 38.2 ou 38.3;
(b) préciser tout ce que l’article 38.2 mentionne comme étant prescrit ou exigé dans les règlements.

Portée générale ou particulière

(2) Les règlements pris en application du présent article peuvent avoir une portée générale ou ne s’appliquer qu’à des personnes, objets ou catégories particuliers.

Catégories

(3) Une catégorie visée dans les règles pris en application du présent article peut être décrite selon n’importe quelle caractéristique ou combinaison de caractéristiques, et peut être décrite comme une catégorie in-
COMMENCEMENT AND SHORT TITLE

Commencement

4. This Act comes into force on the day it receives Royal Assent.

Short title

5. The short title of this Act is the Education Statute Law Amendment Act (Electronic Sexual Material), 2009.

ENTRÉE EN VIGUEUR ET TITRE ABRÉGÉ

Entrée en vigueur

4. La présente loi entre en vigueur le jour où elle reçoit la sanction royale.

Titre abrégé

5. Le titre abrégé de la présente loi est Loi de 2009 modifiant des lois en ce qui a trait à l’éducation (documents électroniques à caractère sexuel).
# LPL Internet Service Action Plan

<table>
<thead>
<tr>
<th>Item/Location</th>
<th>Milestone</th>
<th>Completion date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development</td>
<td>Approval by Library Board</td>
<td>Nov. 19</td>
</tr>
<tr>
<td>Implementation</td>
<td>Commence process to enact policy</td>
<td>Commence Nov. 20</td>
</tr>
<tr>
<td>Implementation</td>
<td>Post policy on website along with communiqué</td>
<td></td>
</tr>
<tr>
<td><strong>External Communications</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Community Stakeholders, including partners</td>
<td>Develop communications strategy for community stakeholders</td>
<td>Nov. 19</td>
</tr>
<tr>
<td></td>
<td>Develop communiqué and FAQ</td>
<td>Nov. 19</td>
</tr>
<tr>
<td></td>
<td>Implement communications strategy</td>
<td>Commence Nov. 20</td>
</tr>
<tr>
<td><strong>Practices/Tools</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action Plan Leadership Team</td>
<td>Identify team and sub teams</td>
<td>Nov. 19</td>
</tr>
<tr>
<td></td>
<td>Convene teams</td>
<td>Nov. 28</td>
</tr>
<tr>
<td><strong>Staff Training</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Orient Coordinators &amp; Supervisors to changes in policy and action plan</td>
<td>Nov. 28 Thru Dec. 10</td>
</tr>
<tr>
<td></td>
<td>Identify and convene “Staff Tools and Training” needs team</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Review and adjust staff procedures and job aids</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Develop FAQ for staff</td>
<td></td>
</tr>
<tr>
<td><strong>Technical Environment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify by IP computers that will be changed and track changes</td>
<td>Dec. 5 (Central) Jan. 31</td>
</tr>
<tr>
<td></td>
<td>Identify and purchase privacy devices as required, e.g. monitor hoods, screens</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ensure that filtering is adjusted on an “as we go basis” by locations</td>
<td>Feb. 28</td>
</tr>
<tr>
<td><strong>Physical Environment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify and convene “Assessment &amp; Rollout” Team: IT, Facilities, Mgrs, Tech Coordinators, location Supervisor/staff</td>
<td>Nov. 19</td>
</tr>
<tr>
<td></td>
<td>Establish Assessment guidelines &amp; criteria</td>
<td>Dec. 5</td>
</tr>
<tr>
<td><strong>Customer Communications</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Review and update public brochures</td>
<td>Dec. 15</td>
</tr>
<tr>
<td></td>
<td>Prepare specific information for parents</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide FAQ on website</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ensure updated feedback mechanisms are in place for Internet service issues: “How did we do today” “Incident Report” “Net Alerts”</td>
<td></td>
</tr>
</tbody>
</table>
# LPL Internet Service Action Plan

## Signage

- Develop consistent signage messaging re: customer responsibilities
- Determine and prepare appropriate format as required by location (hanging, desk)
- Develop on-screen messaging re: responsible viewing

## Sequenced Assessment and Roll Out

<table>
<thead>
<tr>
<th>Location</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Central Library</strong></td>
<td>Dec. 15/08</td>
</tr>
<tr>
<td>Cyber Central, 2nd floor</td>
<td></td>
</tr>
<tr>
<td>Children’s Library</td>
<td></td>
</tr>
<tr>
<td>Teen Annex</td>
<td></td>
</tr>
<tr>
<td>Discover Place</td>
<td></td>
</tr>
<tr>
<td>Training Rooms</td>
<td></td>
</tr>
<tr>
<td><strong>Large Branches</strong></td>
<td>Jan. 31/09</td>
</tr>
<tr>
<td>Masonville</td>
<td></td>
</tr>
<tr>
<td>Byron</td>
<td></td>
</tr>
<tr>
<td>Beacock</td>
<td></td>
</tr>
<tr>
<td>Jalna</td>
<td></td>
</tr>
<tr>
<td><strong>Small Branches</strong></td>
<td>Feb. 14/09</td>
</tr>
<tr>
<td>Northridge</td>
<td></td>
</tr>
<tr>
<td>Lambeth</td>
<td></td>
</tr>
<tr>
<td>Carson</td>
<td></td>
</tr>
<tr>
<td>Glenworth</td>
<td></td>
</tr>
<tr>
<td><strong>Mid-Size Branches</strong></td>
<td>Feb. 28/09</td>
</tr>
<tr>
<td>Cherryhill</td>
<td></td>
</tr>
<tr>
<td>Crouch</td>
<td></td>
</tr>
<tr>
<td>East London</td>
<td></td>
</tr>
<tr>
<td>Landon</td>
<td></td>
</tr>
<tr>
<td>Pond Mills</td>
<td></td>
</tr>
<tr>
<td>Sherwood</td>
<td></td>
</tr>
<tr>
<td>Westmount</td>
<td></td>
</tr>
</tbody>
</table>

## Monitoring/Policy Review

- Monitor and respond to LPL customer feedback
- Continue to monitor policy implementation in locations
- Monitor legislative environment, other libraries

## Wireless Environment

- Monitor impact of wireless and implement due diligence as required

## Policy Review

- Report to Board on policy status
Internet Service Action Plan: Implementation

Staff Training

The Internet Service Policy Action Leadership Team agreed that the following goals were an important component of the implementation plan:

- To review and ensure awareness of the Internet Service Policy
- To understand the rights and obligations of users under the Policy
- To understand the processes and appropriate actions in the event the Policy is contravened by a user

Training Process

In conjunction with the Action Plan Leadership Team, an e-learning module was developed and distributed to staff. The e-learning module included a slide presentation, a procedure document and a laminated job aid for staff.

E-Learning Module

The module outlined the provisions of the Policy and noted the changes. The rights of Users were articulated, and links provided to the appropriate pieces of legislation. The responsibilities of staff were outlined, including processes to follow in the event a user opts to disregard the Policy.

Procedure Document

The document, Procedures for Handling Problems Related to Internet Service, was updated and outlines the responsibilities of staff and offers a variety of potential scenarios with instructions for their successful resolution.

Job Aid

Each department was provided with a laminated sheet that outlines the process and words to use in the event a patron lodges a complaint about another user.

The information was distributed. Public Service Supervisors were required to ensure all staff reviewed the material and to communicate back to the Manager, Training and Development, when it was completed.

Technical Environment

- Monitors of Internet computers checked for privacy screens and replaced as necessary.
- Additional privacy options researched (e.g. monitor hoods, sunken monitor workstations), purchasing some for trial purposes. Products did not noticeably reduce visibility of content on computer screens for walk-by traffic. Staff continues to seek improved technical solutions.
- IT staff worked with the APLT to review individual workstations and to adjust filtering as required; filtering software application reviewed and adjusted for children’s and teen’s areas in all locations.
- In some high traffic areas in branch locations (e.g. Pond Mills) other locations workstations were filtered where other physical and technical solutions were ineffective in reducing visibility of content on computer screens.
- Computer inventory tracking was updated to record filtering changes.

**Physical Environment**

Staff teams reviewed placement and configurations of computer workstations in all Branches and Central Departments.

Placement of all computers in public spaces was reviewed using identified criteria:
- Proximity to children’s, teen areas
- Traffic patterns within location/department
- Level of visibility of on-screen content
- Proximity to staff for service and support
- Staff and public safety, security concerns if placement isolated
- Types of computers (e.g. Express, Catalogue, Research, Internet)
- Physical restrictions or considerations such as wiring, major collection shifts required
- Accessibility requirements in location, computer workstation accessibility

Furniture styles and equipment configurations were assessed.
- Current workstation styles and configurations and placement of privacy side panels inventoried and assessed (e.g. free-standing individual or double rectangular tables, 4-unit pods) for privacy and flexibility; new replacement workstations and privacy panels purchased; workstations switched from one location to another
- Consideration given to use of other physical barriers (e.g. large plants, screens, floor display units and bulletin boards)

As a result of the assessment, revised floor plans were developed and changes were implemented. Public computers are filtered as required by Internet Service Policy. Monitoring, assessment and adjustments are ongoing.
Communications with Users

The Action Plan Leadership Team coordinated the review and revision of current publications, electronic information and signage. As a result:

- Policy brochures are revised, printed and distributed, website and LIBBI updated.
- Internet Safety brochures, *Cyber Danger* and *Take Care to Be Web Aware* are updated and available on website.
- Revised feedback mechanisms are in place, e.g. Net Alerts, “How Did We Do today?”, Incident Reporting (internal form).
- Messaging was added to computer screens as part of login procedure regarding privacy, confidentiality, responsible viewing and appropriate behavior in public places.
- Computer user agreement statement was revised to reflect policy changes.

Sequenced Rollout

The sequenced rollout was completed by March 31, 2009. Ongoing monitoring of policy implementation in terms of physical and technical environments continues.
## Internet Service Incidents, 2008-2009

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Information</th>
<th>Policy/ Guidelines associated</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 29</td>
<td>East London</td>
<td>Patron reported seeing objectionable content on a filtered and unfiltered computer</td>
<td></td>
<td>Problem with sightlines that have been addressed by changing physical layout of Internet computers.</td>
</tr>
<tr>
<td>Mar 13</td>
<td>Central</td>
<td>Patron viewing objectionable content on an ERC computer</td>
<td>ERC computer use guidelines</td>
<td>Staff informed patron of ERC computers use guidelines. ERC computers are for job search purposes only.</td>
</tr>
<tr>
<td>Mar 15</td>
<td>Central</td>
<td>Patron who did not log in properly (with own library card) viewing objectionable content</td>
<td>Computer Use guidelines</td>
<td>Informed of the Computer Use Guidelines. Patrons are required to use their own valid library cards.</td>
</tr>
<tr>
<td>Mar 20</td>
<td>Central</td>
<td>Patron logging in with someone else’s card. Complaint re: viewing objectionable content</td>
<td>Computer Use guidelines</td>
<td>Informed of the Computer Use Guidelines. Patrons are required to use their own valid library cards.</td>
</tr>
<tr>
<td>Mar 22</td>
<td>Central</td>
<td>Patron who did not log in properly (with own library card) viewing objectionable content</td>
<td>Computer Use guidelines</td>
<td>Informed of the Computer Use Guidelines. Patrons are required to use their own valid library cards.</td>
</tr>
<tr>
<td>April 25</td>
<td>Central</td>
<td>Complaint re: viewing objectionable content and alleged inappropriate touching in a public place</td>
<td>Code of Conduct</td>
<td>Patron informed of complaint. Given warning as per policy.</td>
</tr>
<tr>
<td>Date</td>
<td>Location</td>
<td>Information</td>
<td>Policy/ Guidelines associated</td>
<td>Response</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>May 04</td>
<td>Central</td>
<td>Complaint received re: alleged inappropriate touching in a public place</td>
<td>Code of Conduct</td>
<td>Security asked patron to leave. Given warning as per policy. Police were notified. *Since these infractions, the Code of Conduct was reviewed. For this infraction the Police now are called immediately.</td>
</tr>
<tr>
<td>May 14</td>
<td>Central</td>
<td>Complaint viewing objectionable content in Teen Annex and patron had not logged in properly using his library card</td>
<td>Internet Use Policy; Computer Use Guidelines</td>
<td>Patron informed that he is required to use his own library card and the restrictions on computers in the Teen Annex</td>
</tr>
<tr>
<td>July 8</td>
<td>Cherryhill</td>
<td>Confrontation between two patrons re: what was felt to be inappropriate internet viewing by one of the patrons.</td>
<td>Rules of Conduct</td>
<td>Staff explained to the patrons the expected behavior (no shouting and arguing)</td>
</tr>
<tr>
<td>July 10</td>
<td>Crouch</td>
<td>Complaint re: viewing of objectionable content on filtered computer</td>
<td></td>
<td>Staff talked with patron and patron was viewing a video on YouTube</td>
</tr>
<tr>
<td>Dec 8</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable content on ERC computer</td>
<td>ERC Use Guidelines</td>
<td>Patron banned for several infractions.</td>
</tr>
</tbody>
</table>

**Total 2008 : 11**
<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Information</th>
<th>Policy/ Guidelines associated</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 6</td>
<td>Masonville</td>
<td>complaint re: viewing of objectionable content</td>
<td></td>
<td>Sightline problems that have been addressed in physical layout of computers.</td>
</tr>
<tr>
<td>April 7</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable content on an ERC computer</td>
<td>ERC Use Guidelines</td>
<td>Staff explained that ERC computers are for job search purposes only.</td>
</tr>
<tr>
<td>April 22</td>
<td>Central</td>
<td>Complaint re: content on personal laptops using “LimeWire”</td>
<td></td>
<td>IT staff followed up re: file sharing protocol involved and met with patrons.</td>
</tr>
<tr>
<td>May 19</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable content on an ERC computer</td>
<td>ERC Use Guidelines</td>
<td>Staff explained that ERC computers are for job search purposes only.</td>
</tr>
<tr>
<td>May 20</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable content on an ERC computer</td>
<td>ERC Use Guidelines</td>
<td>Staff explained that ERC computers are for job search purposes only.</td>
</tr>
<tr>
<td>May 22</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable content on an ERC computer</td>
<td>ERC Use Guidelines</td>
<td>Staff explained that ERC computers are for job search purposes only.</td>
</tr>
<tr>
<td>May 28</td>
<td>Beacock</td>
<td>Complaint re: viewing of objectionable content on filtered Homework computer</td>
<td></td>
<td>Staff confirmed that the computer was filtered. Staff spoke to the patron involved and reminded in a public area.</td>
</tr>
<tr>
<td>June 9</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable content</td>
<td></td>
<td>Staff reminded patron that he was in a public place. Patron apologized.</td>
</tr>
</tbody>
</table>
### Internet Service Incidents, 2008-2009

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Information</th>
<th>Policy/ Guidelines associated</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 17</td>
<td>Beacock</td>
<td>Complaint re: viewing of objectionable content on 20 minute Express computers</td>
<td></td>
<td>Problem was a sightline issue. Placement of the computers reviewed and physical placement changed.</td>
</tr>
<tr>
<td>Aug 17</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable content</td>
<td></td>
<td>Patron filled out comment card. Staff unable to talk to computer user because the concern was reported after patron had left. Patron called Administration. Policies explained.</td>
</tr>
<tr>
<td>Sept 3</td>
<td>Landon</td>
<td>Complaint re: viewing of objectionable content</td>
<td></td>
<td>Staff member reminded patron that he is in a public place. He apologized and stopped his computer session.</td>
</tr>
<tr>
<td>Sept 5</td>
<td>Byron</td>
<td>Complaint re: viewing of objectionable content on 20 minute computers</td>
<td></td>
<td>Staff member reminded patron that he is in public place.</td>
</tr>
<tr>
<td>Sept 17</td>
<td>Central</td>
<td>Patron in passing reported questionable viewing</td>
<td></td>
<td>Staff reminded patron that he is in a public place. Patron logged off and left.</td>
</tr>
<tr>
<td>Sept 26</td>
<td>Central</td>
<td>Patron using ERC computer to print objectionable images</td>
<td>ERC Use guidelines</td>
<td>Patron asked by staff to leave the area. Computers for job search purposes only.</td>
</tr>
<tr>
<td>Date</td>
<td>Location</td>
<td>Information</td>
<td>Policy/Guidelines associated</td>
<td>Response</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Oct 1</td>
<td>Central</td>
<td>Complaint from visitors to Pillar office re: viewing objectionable content on computer in the area</td>
<td></td>
<td>Patron left before the incident was reported.</td>
</tr>
<tr>
<td>Oct 5</td>
<td>Central</td>
<td>Complaint from Pillar staff re: viewing of objectionable images</td>
<td></td>
<td>Staff reminded patron that he is in a public place and what he is viewing might be inappropriate to the setting.</td>
</tr>
<tr>
<td>Oct 6</td>
<td>Central</td>
<td>Complaint from Pillar staff re: viewing of objectionable images</td>
<td></td>
<td>Staff reminded patron that he is in a public place and what he is viewing might be inappropriate to the setting.</td>
</tr>
<tr>
<td>Oct 6</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable images</td>
<td></td>
<td>Staff reminded patron that he is in a public place and what he is viewing might be inappropriate to the setting.</td>
</tr>
<tr>
<td>Oct 7</td>
<td>East London</td>
<td>Complaint re: viewing of objectionable images</td>
<td></td>
<td>Problem with sightlines that have been addressed by changing physical layout of Internet computers. Discovered a problem with equipment. Problem has been addressed.</td>
</tr>
<tr>
<td>Oct 21</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable images</td>
<td></td>
<td>Staff reminded patron that he is in a public place and what he is viewing might be inappropriate to the setting.</td>
</tr>
<tr>
<td>Oct 22</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable images</td>
<td></td>
<td>Staff reminded patron that he is in a public place and what he is viewing might be inappropriate to the setting.</td>
</tr>
<tr>
<td>Date: 2009 Current policy</td>
<td>Location</td>
<td>Information</td>
<td>Policy/ Guidelines associated</td>
<td>Response</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------</td>
<td>-------------</td>
<td>-------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Oct 23</td>
<td>Westmount</td>
<td>Complaint re: alleged inappropriate touching in a public place</td>
<td>Code of Conduct</td>
<td>Incident was not reported until hours later. The patron involved had left by this time. If report had been made at the time of the incident, staff would have called the Police.</td>
</tr>
<tr>
<td>Nov 9</td>
<td>Central</td>
<td>Complaint re: viewing of objectionable images</td>
<td></td>
<td>The patron had left by the time the staff were notified.</td>
</tr>
</tbody>
</table>

2009 Total to Nov13, 2009 : 24
<table>
<thead>
<tr>
<th>Date</th>
<th>Medium</th>
<th>Issue</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept 18 2009</td>
<td>How Did We Do Today?</td>
<td>Exposed to viewing of sexual images; against viewing pornography</td>
<td>Email response</td>
</tr>
<tr>
<td>Sept 18 2009</td>
<td>How Did We Do Today?</td>
<td>Against viewing of child/adult pornography</td>
<td>Email response</td>
</tr>
<tr>
<td>Oct 2 2009</td>
<td>Telephone</td>
<td>Questions about access to pornography</td>
<td>Telephone call</td>
</tr>
<tr>
<td>Oct 1 2009 &amp;</td>
<td>Email</td>
<td>Exposed to viewing of sexual images; against viewing of child</td>
<td>Email response</td>
</tr>
<tr>
<td>Sept 18 2009</td>
<td></td>
<td>pornography</td>
<td></td>
</tr>
<tr>
<td>Oct 8 2008</td>
<td>Email</td>
<td>Against viewing of pornography</td>
<td>Email response</td>
</tr>
<tr>
<td>Oct 8 2009</td>
<td>Email</td>
<td>Against removal of filters</td>
<td>Email response</td>
</tr>
<tr>
<td>Oct 8 2009</td>
<td>Email</td>
<td>Exposed to viewing of pornography at East London</td>
<td>Email response; review and change of workstation placement</td>
</tr>
<tr>
<td>Oct 9 2009</td>
<td>How Did We Do Today?</td>
<td>Against filtering</td>
<td>Email response</td>
</tr>
<tr>
<td>Oct 9 2009</td>
<td>Email</td>
<td>Against viewing of pornography</td>
<td>Reported by staff through Incident Report Email response</td>
</tr>
<tr>
<td>Oct 14 2009</td>
<td>Email</td>
<td>Against viewing sexual content in a public place with children present</td>
<td>Email response</td>
</tr>
<tr>
<td>Oct 19 2009</td>
<td>Email</td>
<td>Against viewing pornography in “family friendly” place</td>
<td>Email response</td>
</tr>
<tr>
<td>Oct 27 2009</td>
<td>Email</td>
<td>Against viewing sexual content in a public place with children present</td>
<td>Email response</td>
</tr>
</tbody>
</table>
PURPOSE: London Public Library (LPL) Internet Service is consistent with its Vision, Mission, Value Promise and Service Excellence Model. LPL offers Internet access to library customers in an effort to meet community needs in the areas of: Literacy; Learning; Culture, Leisure and Recreation; Information; and Community Meeting Place.

The purpose of this policy is to outline: Library responsibilities in providing this public service; library use of filters; user responsibilities in accessing LPL Internet Service; staff responsibilities; and consequences of inappropriate behaviour or illegal activity by users.

DEFINITIONS:

Internet is a worldwide interconnected network of computers that allows the "sharing" or "networking" of information at remote sites from other academic institutions, research institutes, private companies, government agencies, and individuals.

SCOPE:

As part of its suite of services to the public, LPL offers Internet Service. From LPL’s point of view, the Internet is the ideal vehicle to:

- Enhance public access to global information and expressions of creativity and thought;
- Expand the library’s collection of information resources;
- Provide users with the opportunity for remote dialogue with subject-matter experts and to engage with other people on an infinite variety of topics; and
- Enable collaborative research and study.

LPL recognizes that in addition to the many valuable resources available on the Internet, some resources are illegal, misleading and/or inaccurate. Others may be considered by some people to be offensive, objectionable and/or intimidating.

In provision of access to content and communication media through its Internet Service, LPL will act in accordance with the Canadian Charter of Rights and Freedoms which states that everyone has freedom of thought, belief, opinion and expression.
Appendix 7

LONDON PUBLIC LIBRARY
POLICY

Title: Internet Service Policy
Policy Category: Means
Policy No.: B-M-009
Issuing Date: November 19, 2008

LPL will support the Canadian Copyright Act and other laws governing intellectual property; the Criminal Code of Canada and other legislation governing access to and communication of information, knowledge, opinion, creative thought and intellectual activity; and privacy legislation.

LPL will develop and implement Internet service policies, guidelines and procedures, under the authority of the Public Libraries Act and in accordance with the LPL Vision, Mission, Value Promise and Service Excellence Model.

POLICY STATEMENT:

1. Library Responsibilities

LPL will proactively facilitate and promote public access to quality information for all users, through various means such as information and referral services so that people may benefit from the use of the Internet.

LPL will proactively promote user education, media awareness and Internet safety.

LPL will respect the right of users to privacy and confidentiality with regards to information sought or received and resources consulted, acquired or transmitted.

In respect of the range of sensibilities and viewpoints of its diverse clientele, LPL will endeavour to minimize the opportunity for unintentional exposure by people using library space to content being accessed by another library user.

Due to the constraints/limitations of space at library locations, LPL will advise users that they are in a public space and will encourage all users to be respectful of the rights and sensibilities of others.

LPL will support the right and responsibility of parents or legal guardians to determine, monitor and guide their children’s use of library materials and resources. The Library does not act in place of or in the absence of a parent. LPL will endeavour to proactively support children, parents and guardians in safe use of the Internet.

LPL will endeavour to minimize unintentional exposure by children and teens to Internet content that is age inappropriate. LPL tailors physical and virtual environments to support the
needs and expectations of children and teens. LPL will ensure Internet services in such spaces facilitate and promote appropriate access.

2. Internet Filtering

LPL will not limit access to Internet content except as outlined below.

The London Public Library will filter the following categories of computers:

- Computers specifically designated for use by children and/or teens, such as Homework Centres;
- Computers in spaces specifically designed for use by children and/or teens; and
- Computers designated for specific functions, such as the Employment Resource Centre computers.

LPL will encourage user awareness that filters are not 100% effective. The Library assumes no liability in the event that a user reaches a site assumed to be filtered.

3. User Responsibilities

Users are responsible for any access points they reach and appropriate use of the resource.

Users are responsible for determining the reliability, currency and accuracy of sites accessed and information found using the Internet.

All customers of London Public Library, including those using the Library's Internet services, are responsible for following the Library's Charter of Use and Rules of Conduct which are designed to provide a welcoming and safe environment for the enjoyment of the public and staff so that all persons may enjoy the benefits of the Library.

Users are responsible for respecting the rights of others when accessing Internet sites in library space. Users must be aware that library computer workstations are in public areas shared by people of all ages and sensibilities. Some content is age inappropriate for children. Some content may be offensive, objectionable and/or intimidating to other Library customers and/or staff.
Users are responsible for respecting the privacy of other library customers.

Users are responsible for determining the legality of any sites they access. Users are subject to federal, provincial and municipal legislation regulating Internet use and must not use the Internet for illegal purposes including copyright violation, obscenity, child pornography, sedition and the incitement of hate. The use of the Library’s Internet services for illegal purposes is prohibited.

Users must be aware that the Internet is not a secure medium and that third parties may be able to obtain information about their activities or themselves. Users are responsible for any fees, losses or damages that occur as a result of any online transactions they conduct on the Internet. The Library assumes no responsibility for the security and privacy of online transactions.

4. Staff Responsibilities

LPL staff are active intermediaries between users and Internet resources and are essential to the provision of relevant, accessible, high quality library services. Staff will support the user in effective, efficient and responsible use of the library Internet service. Staff can help users determine the reliability, currency and accuracy of sites accessed and information found using the Internet.

Staff do not monitor nor censor content.

Library staff are entrusted with the obligation to ensure that all rules of computer use and Internet service are followed. Staff will advise customers of appropriate conduct as required and state consequences of not following the rules of conduct should unacceptable behaviour continue or be repeated.

5. Consequences of Misuse of the LPL Internet Service

The Library will take action on any inappropriate behaviours related to use of the LPL Internet Service, such as intimidation, harassment, bullying, etc., according to the library’s Code of Conduct.

LPL will take action in a situation where unlawful activity occurs, and will contact the police. For legal reasons, complaints from patrons that a user is accessing legally prohibited material may also result in LPL contacting the police.

Any person violating Library rules for Internet Service risks suspension of Library privileges,
exclusion from the Library for a period of time, banning and/or prosecution.

INQUIRIES:

Manager, Services and Operations
Chief Executive Officer

KEYWORDS:

RELATED DOCUMENTS:

Charter of Library Use: Rules of Conduct
Charter of Library Use: Unattended Children
Privacy Policy

DOCUMENT CONTROL:

Approved: January 26, 1997
Revised: September 24, 1997
March 25, 1998
September 26, 2001
November 21, 2007
November 19, 2008
First Session, Fortieth Parliament,
57 Elizabeth II, 2008

HOUSE OF COMMONS OF CANADA

BILL C-209

An Act to prevent the use of the Internet to distribute pornographic material involving children

FIRST READING, NOVEMBER 21, 2008

NOTE

2nd Session, 40th Parliament
This bill was introduced during the First Session of the 40th Parliament. Pursuant to the Standing Orders of the House of Commons, it is deemed to have been considered and approved at all stages completed at the time of prorogation of the First Session. The number of the bill remains unchanged.

MR. STOFFER

401035

SUMMARY

This enactment provides for the licensing of Internet service providers by the Canadian Radio-television and Telecommunications Commission (CRTC) on conditions to be set by the Minister of Industry by regulation. It also requires service providers to co-operate in minimizing the use of the Internet for the publication or proliferation of child pornography or the facilitation of a sex offence involving a child.

Anyone who uses the Internet to facilitate any of the designated sex offences involving children is guilty of an offence.

Internet service providers may be required to block access to identified portions of the Internet that carry child pornography.

The Minister may enter into agreements with provinces or foreign states to assist in achieving the purposes of the Act. Special powers under search warrants may be prescribed by the Minister to facilitate electronic searches.

Also available on the Parliament of Canada Web Site at the following address:

http://www.parl.gc.ca
"designated offence involving a child" means an offence under any of the following provisions of the Criminal Code, where the victim was 14 years of age or more but under the age of 18 years at the time of the commission of the offence, and the offender was in a position of trust or authority towards the victim or was a person with whom the victim was in a relationship of dependency or where the victim was under the age of 14 years at the time of the commission of the offence:

(a) section 151 (sexual interference);  
(b) section 152 (invitation to sexual touching);  
(c) section 153 (sexual exploitation);  
(d) section 155 (incest);  
(e) section 159 (anal intercourse);  
(f) subsection 160(2) or (3) (compelling commission of bestiality or bestiality in presence of or by child);  
(g) section 170 (parent or guardian procuring sexual activity);  
(h) section 172 (corrupting children);  
(i) subsection 173(2) (exposure to person under age of 16 years);  
(j) section 271 (sexual assault);  
(k) section 272 (sexual assault with a weapon, threats to a third party or causing bodily harm); and  
(l) section 273 (aggravated sexual assault).

"Internet service provider" means a person who provides a service that facilitates access to the Internet, whether or not the service is provided free or for a charge.

"Minister" means the Minister of Industry.

"prescribed" means prescribed by regulation.

"subscriber" means a person who contracts with or uses the services of an Internet service provider to obtain access to the Internet.

**PURPOSE**

3. The purpose of this Act is to prevent the use of the Internet to unlawfully promote, display, describe or facilitate participation in unlawful sexual activity involving young persons.

**LICENCE**

3. La présente loi a pour objet d'interdire le recours à Internet pour promouvoir, représenter ou décrire illégalement des activités sexuelles illicites impliquant des enfants ou pour faciliter la participation à de telles activités.

**Licence**

Service providers licensed

4. (1) No person shall offer the services of, or operate as, an Internet service provider unless the person has been granted a licence to operate as an Internet service provider in accordance with subsection (2).

Granting a licence

2) The Commission shall grant a licence to operate as an Internet service provider to any applicant who meets the prescribed requirements and who has submitted to the Commission
(a) an application in the prescribed form and manner; and
(b) a written undertaking to report the prescribed information in accordance with the regulations.

Licence cancelled

3) The Commission may cancel a licence granted under subsection (2) if the licensee or, where the licensee is a corporation, a director or officer of the corporation is convicted of an offence under section 163.1 of the Criminal Code or a designated offence involving a child, or commits an offence under this Act.

PROHIBITION

5. (1) No Internet service provider shall knowingly permit the use of its service
(a) for placing child pornography on the Internet or for viewing, reading, copying or retrieving child pornography from the Internet;
(b) by any person who the provider knows has been convicted of an offence under this Act within the previous seven years; or
(c) by any person who the provider knows has used the Internet within the previous seven years for a purpose that would be an offence under this Act.

Use of Internet for child pornography

2) No person shall place child pornography on the Internet for the purpose of communicating it to another person or making it accessible to another person for viewing, reading, copying or retrieval, whether such access is open or restricted by any means.

Possession of pornography from Internet

3) No person shall possess any child pornography retrieved from the Internet.

Use of Internet to contact person

4) No person shall use the Internet to contact a person for the purpose of facilitating a designated offence involving a child.

4. (1) Nul ne peut offrir des services de fournisseur d'accès Internet ou exploiter une entreprise offrant ces services s'il n'a obtenu une licence pour exploiter une entreprise de services d'accès Internet conformément au paragraphe (2).

2) Le Conseil délivre une licence pour exploiter une entreprise offrant des services de fournisseur d'accès Internet à tout demandeur qui répond aux exigences réglementaires et qui a soumis au Conseil :
(a) une demande selon la procédure et la forme réglementaires;
(b) un engagement écrit de fournir les renseignements réglementaires conformément aux règlements.

3) Le Conseil peut annuler la licence délivrée aux termes du paragraphe (2) si le titulaire — ou un dirigeant ou un administrateur du titulaire, si celui-ci est une personne morale — est déclaré coupable d'une infraction à l'article 163.1 du Code criminel ou d'une infraction désignée concernant un enfant, ou s'il commet une infraction à la présente loi.

INTERDICATION

5. (1) Il est interdit à tout fournisseur d'accès Internet de permettre sciemment que ses services :
(a) servent à la diffusion, la visualisation, la lecture, la reproduction ou la récupération de pornographie juvénile par Internet;
(b) soient utilisés par une personne qu'il sait avoir été reconnue coupable d'une infraction à la présente loi au cours des sept années précédentes;
(c) soient utilisés par une personne qu'il sait avoir utilisé Internet au cours des sept années précédentes à des fins qui seraient considérées comme une infraction à la présente loi.

Diffusion de pornographie juvénile dans Internet

2) Nul ne peut diffuser de la pornographie juvénile dans Internet pour la communiquer à quelqu'un ou pour permettre à quelqu'un de la visualiser, la lire, la reproduire ou la récupérer, que l'accès en soit libre ou restreint de quelque façon.

Possession de pornographie juvénile provenant d'Internet

3) Il est interdit de posséder de la pornographie juvénile provenant d'Internet.

Utilisation d'Internet pour contacter une personne

4) Il est interdit de contacter par Internet une personne en vue de faciliter la perpétration d'une infraction désignée concernant un enfant.

(5) No person shall respond to a contact that is made using the Internet for the purpose of facilitating a designated offence involving a child.

OFFENCE

6. (1) A person who contravenes subsection 5(1), (2), (3), (4) or (5) is guilty of an offence and liable on summary conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding two years, or to both.

Directors and officers

(2) A director or officer of a corporation that commits an offence under subsection (1) who is aware of the circumstances on which the offence is based before it is committed, or becomes aware of them while it is being committed, is also guilty of the offence and liable to the punishments provided in subsection (1).

(3) An Internet service provider is not guilty of an offence under subsection (1) if, immediately after becoming aware that a person is using its service to commit an offence under this Act, the provider

(a) terminates its service to that person;

(b) takes all reasonable steps to remove or prevent access to any material unlawfully placed on the Internet by that person; and

(c) advises the Minister of the identity of that person, the nature of the material and the means whereby it may be accessed by others.

7. The Minister may order an Internet service provider to use all means that are reasonably available to the Internet service provider to prevent access by its subscribers to any material on the Internet that the Minister, after reasonable inquiry, determines to be child pornography.

Offence and penalty

8. (1) An Internet service provider who refuses or fails to comply with an order made under section 7 is guilty of an offence and liable on summary conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding one year, or to both.

Directors and officers

(2) A director or officer of a corporation that is an Internet service provider that commits an offence under subsection (1) is also guilty of the offence and liable to the

INFRINGEMENT

6. (1) Toute personne qui contravient aux paragraphes 5(1), (2), (3), (4) ou (5) est coupable d’une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d’une amende maximale de 100 000 $ et d’un emprisonnement maximal de deux ans, ou de l’une de ces peines.

(2) Tout administrateur ou dirigeant d’une personne morale qui a connaissance des circonstances dans lesquelles cette personne morale commet une infraction au paragraphe (1), avant qu’elle soit commise ou pendant qu’elle est commise, est lui-même coupable de l’infraction et passible des peines prévues à ce paragraphe.

(3) N’est pas coupable d’une infraction visée au paragraphe (1) le fournisseur d’accès Internet qui apprend qu’une personne utilise ses services pour commettre une infraction à la présente loi et qui, sans tarder :

(a) interrompt ses services auprès de cette personne;

(b) prend toutes les mesures raisonnables pour supprimer d’Internet tout document qui s’y trouve illégalement ou pour en interdire l’accès;

(c) informe le ministre de l’identité de la personne, de la nature du document et des moyens d’accès dont d’autres peuvent disposer.

7. Le ministre peut ordonner au fournisseur d’accès Internet de prendre tous les moyens raisonnables à sa disposition pour empêcher les abonnés d’avoir accès à tout document qui se trouve dans Internet et que le ministre déclare, après enquête raisonnable, être de la pornographie juvénile.

8. (1) Tout fournisseur d’accès Internet qui refuse ou omet de se conformer à l’ordre donné en vertu de l’article 7 est coupable d’une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d’une amende maximale de 50 000 $ et d’un emprisonnement maximal d’un an, ou de l’une de ces peines.

(2) Tout administrateur ou dirigeant d’une personne morale qui est un fournisseur d’accès Internet et qui commet une infraction au paragraphe (1) est lui-même coupable.
punishments provided in subsection (1).

AGREEMENTS

9. The Minister may enter into agreements with a province or a foreign state relating to the exchange of information and co-operation to prevent or minimize the use of the Internet for the publication or proliferation of child pornography or for facilitating the commission of an offence under the Criminal Code or this Act or a similar law of the province or foreign state.

WARRANTS

10. (1) The Minister may prescribe any special powers that are reasonably necessary in the opinion of the Minister to facilitate searches of electronic data or systems or storage in the execution of a search warrant issued under section 487 of the Criminal Code in respect of an offence or suspected offence under this Act.

(2) A warrant conferring any powers prescribed under subsection (1) is subject to the same principles respecting authorization and grounds for suspicion as, and to the procedures and conditions required in respect of, a search warrant under the Criminal Code.

REGULATIONS

11. The Minister may make regulations prescribing

(a) the form and manner of making an application for a licence under section 4;
(b) any financial and technical resources that an applicant must show to the Commission in order to be granted a licence under section 4;
(c) any information that a person who is granted a licence under section 4 is required to report to the Commission for the purposes of this Act;
(d) any special powers that may be conferred by a search warrant for the purposes of subsection 10(1); and
(e) anything that by this Act is to be prescribed.
HOUSE OF COMMONS OF CANADA

BILL C-58

An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service

FIRST READING, NOVEMBER 24, 2009

MINISTER OF JUSTICE

90543

SUMMARY

This enactment imposes reporting duties on persons who provide an Internet service to the public if they are advised of an Internet address where child pornography may be available to the public or if they have reasonable grounds to believe that their Internet service is being or has been used to commit a child pornography offence. This enactment makes it an offence to fail to comply with the reporting duties.

Also available on the Parliament of Canada Website at the following address:
http://www.parl.gc.ca

TABLE OF PROVISIONS

AN ACT RESPECTING THE MANDATORY REPORTING OF INTERNET CHILD PORNOGRAPHY BY PERSONS WHO PROVIDE AN INTERNET SERVICE

SHORT TITLE
1. Child Protection Act (Online Sexual Exploitation)

INTERPRETATION
2. Definitions

DUTIES
3. Duty to report Internet address

An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service

Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows:

SHOR T TITLE
1. This Act may be cited as the Child Protection Act (Online Sexual Exploitation).

INTERPRETATION
2. (1) The following definitions apply in this Act.

"child pornography": has the same meaning as in subsection 163.1(1) of the Criminal Code.

"child pornography offence": means an offence under any of the following provisions of the Criminal Code:
(a) subsection 163.1(2) (making child pornography);
(b) subsection 163.1(3) (distribution, etc., of child pornography);
(c) subsection 163.1(4) (possession of child pornography);
(d) subsection 163.1(4.1) (accessing child pornography).

"computer data": means representations, including signs, signals or symbols, that are in a form suitable for processing in a computer system.

"Internet service": means Internet access, Internet content hosting or electronic mail.

"person": means an individual, a corporation, a partnership or an unincorporated association or organization.

(2) The descriptive words in parentheses that follow the reference to a provision of the Criminal Code in the definition "child pornography offence" in subsection (1) do not form part of that definition but are inserted for convenience of reference only.

PROJET DE LOI C-58

Loi concernant la déclaration obligatoire de la pornographie juvenile sur Internet par les personnes qui fournissent des services Internet

Sa Majesté, sur l'avis et avec le consentement du Sénat et de la Chambre des communes du Canada, édicté :

TITRE ABRÉGÉ
1. Loi sur la protection des enfants (exploitation sexuelle en ligne).

DÉFINITIONS
2. (1) Les définitions qui suivent s'appliquent à la présente loi.

« données informatiques » Représentations, notamment signes, signaux ou symboles, qui sont sous une forme qui en permet le traitement par un ordinateur.

« infraction relative à la pornographie juvenile » Infrac tion à l'une des dispositions ci-après du Code criminel :
(a) paragraphe 163.1(2) (production de pornographie juvenile);
(b) paragraphe 163.1(3) (distribution de pornographie juvenile);
(c) paragraphe 163.1(4) (possession de pornographie juvenile);
(d) paragraphe 163.1(4.1) (accès à la pornographie juvenile).

« personne » Personne physique ou morale, société de personnes ou organisation ou association non dotée de la personnalité morale.

« pornographie juvenile » S'entend au sens du paragraphe 163.1(1) du Code criminel.

« services Internet » Services d'accès à Internet, d'hébergement de contenu sur Internet ou de courrier électronique.

(2) Les mots entre parenthèses qui suivent le renvoi à une disposition du Code criminel dans la définition de « infraction relative à la pornographie juvenile » au paragraphe (1) ne font pas partie de celle-ci et ne sont cités que pour des raisons de commodité.
DUTIES

3. If a person is advised, in the course of providing an Internet service to the public, of an Internet Protocol address or a Uniform Resource Locator where child pornography may be available to the public, the person must report that address or Uniform Resource Locator to the organization designated by the regulations, as soon as feasible and in accordance with the regulations.

4. If a person who provides an Internet service to the public has reasonable grounds to believe that their Internet service is being or has been used to commit a child pornography offence, the person must notify an officer, constable or other person employed for the preservation and maintenance of the public peace of that fact, as soon as feasible and in accordance with the regulations.

Preservation of computer data

5. (1) A person who makes a notification under section 4 must preserve all computer data related to the notification that is in their possession or control for 21 days after the day on which the notification is made.

(2) The person must destroy the computer data that would not be retained in the ordinary course of business and any document that is prepared for the purpose of preserving computer data under subsection (1) as soon as feasible after the expiry of the 21-day period, unless the person is required to preserve the computer data by a judicial order made under any other Act of Parliament or the legislature of a province.

No disclosure

6. A person must not disclose that they have made a report under section 3 or a notification under section 4, or disclose the contents of a report or notification, if the disclosure could prejudice a criminal investigation, whether or not a criminal investigation has begun.

No making use of child pornography

7. Nothing in this Act requires or authorizes a person to seek out child pornography.

Intemalé

8. A civil proceeding cannot be commenced against a person for making a report in good faith under section 3 or for making a notification in good faith under section 4.

Self-incrimination

9. For greater certainty, nothing in this Act affects any right of a person to be protected against self-incrimination.

Preservation of foreign proceedings

10. A person who has reported information in accordance with an obligation to report child pornography under the laws of a province or a foreign jurisdiction is deemed to have complied with this Act in relation to that information.

OFFENCES AND PUNISHMENT

11. Every person who knowingly contravenes any of sections 3 to 6 is guilty of an offence and liable on summary conviction, (a) in the case of an individual,

(i) for a first offence, to a fine of not more than $1,000,
(ii) for a second offence, to a fine of not more than $5,000, and
(iii) for each subsequent offence, to a fine of not more than $10,000 or to imprisonment for a term of not more than six months, or to both; and

(b) in all other cases,

(i) for a first offence, to a fine of not more than $10,000,

OBLIGATIONS

3. La personne qui est avisée, dans le cadre des services Internet qu'elle fournit au public, d'une adresse de protocole Internet ou d'une adresse URL où pourrait se trouver de la pornographie juvenile accessible au public communique l'adresse dans les meilleurs délais, selon les modalités réglementaires, à l'organisme désigné par les règlements.

4. Si la personne qui fournit des services Internet au public a des motifs raisonnables de croire que ses services Internet sont ou ont été utilisés pour la perpétration d'une infraction relative à la pornographie juvenile, elle en avise dans les meilleurs délais, selon les modalités réglementaires, un agent de police ou toute autre personne chargée du maintien de la paix publique.

5. (1) La personne qui a donné l'avis prévu à l'article 4 préserve les données informatiques afferrentes en sa possession ou à sa disposition pendant vingt et un jours après la date de l'avis.

(2) Elle est tenue de détruire les données informatiques qui ne seraient pas conservées dans le cadre normal de son activité commerciale et tout document établi en vue de les préserver en application du paragraphe (1) dans les meilleurs délais après l'expiration des vingt et un jours, à moins qu'elle ne soit assujettie à une ordonnance de préervation rendue en vertu d'une autre loi fédérale ou provinciale à l'égard de ces données.

6. Nul ne peut, si cela est susceptible de nuire à une enquête criminelle en cours ou à venir, révéler qu'il a fait une communication en application de l'article 3 ou donné un avis en application de l'article 4 ou dévoiler leur contenu.

7. La présente loi n'a pas pour effet d'autoriser ou d'obliger quiconque à chercher de la pornographie juvenile.

8. Nul ne peut être poursuivi au civil pour avoir, de bonne foi, communiqué une adresse au titre de l'article 3 ou donné un avis au titre de l'article 4.

9. Il demeure entendu que la présente loi ne porte atteinte à aucun droit de la personne en matière de protection contre l'auto-incrimination.

10. La personne qui communique des renseignements en application de la loi d'une province ou d'un État étranger sur la déclaration obligatoire de la pornographie juvenile est réputée s'être conforme à la présente loi à l'égard de ces renseignements.

INFRACTIONS ET PEINES

11. Qui conçoit ou contrevient sciemment à l'un des articles 3 à 6 commet une infraction et encourt, sur déclaration de culpabilité par procédure sommaire, a) dans le cas d'une personne physique:

(i) pour la première infraction, une amende maximale de mille dollars,
(ii) pour la deuxième infraction, une amende maximale de cinq mille dollars,
(iii) pour chaque récidive subséquente, une amende maximale de dix mille dollars et un emprisonnement maximal de six mois, ou l'une de ces peines;

b) dans les autres cas:

(i) pour la première infraction, une
12. A prosecution for an offence under this Act cannot be commenced more than two years after the time when the act or omission giving rise to the prosecution occurred.

13. The Governor in Council may make regulations
(a) designating an organization for the purpose of section 3;
(b) respecting the role, functions and activities of the designated organization in relation to information received under this Act, including any security measures to be taken;
(c) respecting the making of a report under section 3;
(d) respecting a notification under section 4;
(e) respecting security measures to be taken in relation to computer data preserved under section 5; and
(f) generally, for carrying out the purposes and provisions of this Act.

14. This Act comes into force on a day to be fixed by order of the Governor in Council.
Status of the Bill

Bill C-58  An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service

<table>
<thead>
<tr>
<th>House of Commons</th>
<th>Senate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Reading</td>
<td>1st Reading</td>
</tr>
<tr>
<td>November 24, 2009</td>
<td>Debate(s) at 2nd Reading</td>
</tr>
<tr>
<td>2nd Reading</td>
<td>Committee</td>
</tr>
<tr>
<td>Committee</td>
<td>Committee Meeting(s)</td>
</tr>
<tr>
<td>Committee Meeting(s)</td>
<td>Committee Report</td>
</tr>
<tr>
<td>Report Presentation and Debate(s)</td>
<td>Report Presentation and Debate(s)</td>
</tr>
<tr>
<td>Report Stage</td>
<td>Report Stage</td>
</tr>
<tr>
<td>Debate(s) at 3rd Reading</td>
<td>Debate(s) at 3rd Reading</td>
</tr>
<tr>
<td>3rd Reading</td>
<td>3rd Reading</td>
</tr>
</tbody>
</table>

Royal Assent: Statutes of Canada:

In Force: 14. This Act comes into force on a day to be fixed by order of the Governor in Council.

Coming into force information updated to November 26, 2009

Days Debated:
- House of Commons - 1
- Senate -