

Practical Privacy

Building a Culture of Privacy in
Municipal Government

Agenda

- Municipal Sector
- Privacy Challenges
- Privacy Culture
- Building privacy culture into practice

Municipal Sector

- MFIPPA
- PHIPA
- Local Governance: Councillors
- Direct Contact with the Public
- Media Concerns
- Cultural Resistance to Access and Privacy Realities

Privacy Challenges

- Two basic models of privacy administration
 - Strongly Centralized
 - Decentralized
- Combination works best
- A strong central knowledge base
- Diffused information as to practices and policy

Privacy Challenges

- Technology
- Corporate Attitudes towards access and privacy
 - Culture of secrecy
 - Ignorance amongst staff as to their responsibilities
 - Solution by short cut

Building Privacy Culture

- Privacy is a statutory requirement
- Ethical base
- Professional knowledge
- Personally applicable to the employee
- Pride in purpose

Building Privacy Culture Into Municipal Government

- Training
- Simple Guidelines
- Uniform policy
- Expert Contacts
- Privacy Impact Assessments
- Privacy Audits
- More Training

Training

- All staff must have some familiarity with the legislation and their responsibilities to the institution and the public.
- Believe what you are teaching them.
- Adequately define privacy
- Give them examples that relate to their personal lives
- Bring that recognition to their professional lives

Training

- Use as many examples as you can.
- Keep the legalities to a minimum, but where necessary give them the legal definition
- Have standardized policies and practices in place.
- Have guidelines on hand to train from.

Guidelines

- Best practices
- Simple guidelines that come from solid corporate policies-bullet points, single page where necessary
- Uniform forms and letters when dealing with disclosures to law enforcement or legislated investigators
- Train using them

Create Uniform Corporate Policies

- One form for one purpose
- Have a defined corporate access and privacy policy and/or manual
- Have a means of communication to disseminate this among staff, or a central repository where they can be directed.
- Have contact information for expert staff available to staff.

Expert Contact

- Your privacy Officer must be available to staff
- Answer all questions , no matter how inane they might seem at the time.
- Build accessibility and trust into the job description.
- It is better that they ask a question than remain silent.

Privacy Impact Assessments

- The use of PIA's should be standard practice for all initiatives that involve personal information
- PIA's do not have to be large to be effective.
- A review of a form that collects PI would follow the same principles as the normal PIA.

Privacy Audit

- A tool to assess the privacy compliance of an ongoing process. A business unit, division, department.
- Assessing solutions based on the corporate culture.
- Active emplacement of privacy construction while not interrupting the normal business flow.

Consistent Messages

- Train constantly
- Buy in at higher levels
- Public Trust
- Employee Satisfaction

Examples of Present Processes

- 32 Disclosures to Law Enforcement
- Privacy Breaches
- Privacy Complaints
- Best Practices

Section 32

- The most common requests for disclosure of personal information fall under 4 sections.
- subsection b) Consent
- subsection d) Officer/employee
- subsection g) Law Enforcement
- subsection e) Act of Legislature/Parliament



Division:
Unit:
Address:

LAW ENFORCEMENT OFFICER REQUEST FORM: ACCESS TO PERSONAL INFORMATION

The following information is being requested under section 32(g) of the Municipal Freedom of Information and Protection of Privacy Act which allows for the disclosure of records containing personal information for the purposes of aiding a law enforcement investigation.

This section to be completed by City Staff:

Information Requested

Client/Employee Name (circle one):

File Location (Area/District Office):

File/Record Title(s):

Description of Records:

This section to be completed by attending Law Enforcement Officer (including: Toronto Police Services, OPP, RCMP, Correctional Service of Canada, Ontario Ministry of Correctional Services).

Subject Name: _____

Occurrence No. _____ or Warrant of Apprehension No. _____

Review Original Documents: Yes No Copies Requested _____

Original Requested: _____
(release original under subpoena only)

I _____ request the above personal information to aid an investigation undertaken
(Officer)
by _____ with view to a law enforcement proceeding or from which a law
(Law Enforcement Institution)
enforcement proceeding is likely to result.

Signature of Investigating Officer *Badge/Identification No.* *Date*

Signature of Staff Member *Date*

City staff contact name: _____ Phone #: _____

Return all completed ORIGINAL forms to the Corporate Access and Privacy Office, City Clerk's Office, Toronto City Hall, 13th floor, West, Tower, 100 Queen Street West, Toronto, ON, M5H 2N2. Should you have any questions regarding the use of this form, please contact the Director, Corporate Access and Privacy at: 416- 392-9683.

Breaches in the City

- Hannon Preschool Language Learning Centre
- 1200 Children
- TB Diagnosis
- Letter sent to an individual who worked with the diagnosed person.

Managing a Breach

- Contain
- Contact CAP
- Document
- Confirm the Scope
- Identify those effected
- Determine the policies procedures responsible
- Mitigate
- Time is important

Privacy Complaints and Investigations

- Informal
- Formal
- Require an investigation of the circumstances that surround the complaint
- Copy CAP on files and policies surrounding the issue
- Mitigation/defending the City's practices.

Best Practices

- The law provides a ground floor for privacy practices but it doesn't tell us how to protect privacy.
- Best practices serve as policy and guidelines that allow us to put standards and compliance into practice

Sick Kids' laptop theft angers watchdog

- A laptop computer containing the personal health information of 2,900 patients at the Hospital for Sick Children was stolen in January and the Ontario privacy commissioner plans to issue a scathing report tomorrow about the incident. The commissioner, Ann Cavoukian, was made aware of the incident in January and began an investigation.
- It's not clear how long after the incident that the privacy commissioner was contacted.
- The laptop was stolen Jan. 4 from the car of a physician who was doing data analysis.

In the last year

- Laptop with finance data on New York City retirees **stolen** -August 23, 2007
- Sick Kids doctor **loses data** on 3,300 patients April 21, 2007
- Laptop containing D.C. employees' personal data **stolen**-August 2007
- Health laptop **theft**- Capital Health –May 8, 2007
- Computer **stolen** with state tax data for 106,000 residents- August 29, 2007
- State laptop containing personal data is **stolen**- August 31, 2007
- VeriSign worker exits after **laptop security breach** - July 2007
- St Edmundsbury Borough Council **Stolen** Laptop with Payroll Information- 9/15/07
- Attorney General Suing Consulting Company Over **Lost Data** - September 19, 2007
- Laptop **Theft** From Vehicle-June 2007
- **Stolen** laptop prompts security reminder-September 17, 2007
- The password-protected laptop belonging to an Ernst & Young auditor was **taken in late February from a locked car**
- Boeing **laptop theft** puts U.S. data breach tally over 100M-December 2006
- Fraud victim after council **laptop theft** - 27 November 2007

Transporting Information

- Briefcases, laptops, PDA's are frequently stolen.
- Consider the PI you transport as important to you as your own.
- Do not leave it unattended for an instant.

Other Best Practices

- Clean Desk Policy
- Secure Disposal
- Maintaining professional/personal boundaries