REGISTRATION FORM

Toolkit for Change • Access & Privacy Workshop 2005
October 6-7, 2005, Toronto, Ontario

Registration fee: The registration fee of $130.00 (plus GST where applicable) covers all sessions, refreshments and luncheons for the two days. Cancellation with full refund allowable up to two weeks before the workshop, less $25 administration fee, or a replacement delegate may be sent.
Confirmation: All registered delegates will receive a Confirmation email and Breakout Session Selection email before the workshop.
Program materials: An information kit will be available to all delegates upon registration at the workshop. It will include confirmation of Breakout Sessions selections, updated workshop information and an identification badge.

Delegate Name _____

Delegate Title _____

Organization _____

Address _____

City _____ Province _____ Postal Code _____

Phone _____ Fax _____

Email _____

3 Ways to Pay (please indicate one method):

❒ 1. Cheque to follow in mail (Payable to Verney Conference Management)

❒ 2. Invoice me

❒ 3. Visa / MC / Am Ex Card #: _____

Expiry Date: _____ Signature: _____

For further information: Call 613-226-8317 Fax: 613-226-8421
Email: registration@verney.ca
Web: www.governmentevents.ca/apw2005

Payment must be received on or by October 6, 2005. Send completed registration form with cheque or money order payable to :

VERNEY CONFERENCE MANAGEMENT
20 JAMIE AVE., 2ND FLOOR, OTTAWA, ON K2E 6T6
GST REGISTRATION # 865047062

To register, please make a photocopy of this page, complete and fax to 613-226-8421 or register online at www.governmentevents.ca

Verney Conference Management
20 Jamie Avenue, 2nd Floor
Ottawa, ON K2E 6T6

CANADA POSTES
POST CANADA
Postage paid Port payé
Addressed Admail Médiaposte avec adresse
5511852

Sponsored by: Ministry of Government Services

Co-Sponsors: Association of Municipal Clerks & Treasurers of Ontario, FOI Police Network, Information Technology Education Council (ITEC), Municipal Info Systems Association (MISA), Ontario Association of School Business Officials (OASBO)

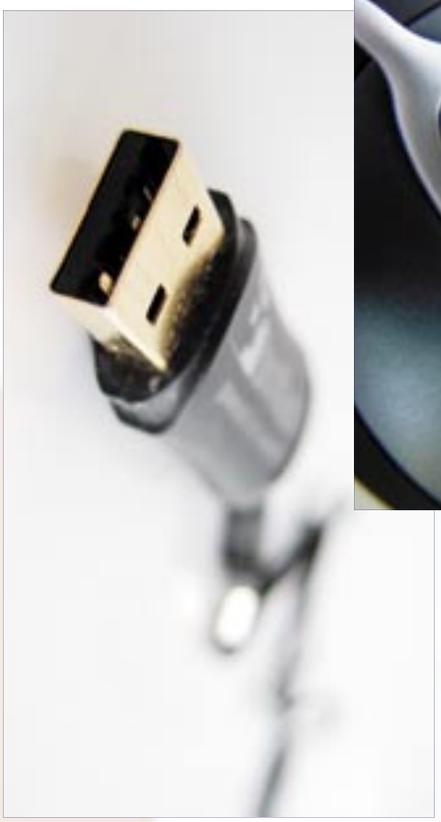
Proposed Topics for Workshop 2005

Working with the IPC	Legal Stream	Operational Privacy Protection	Access & Privacy	Technology	Other Jurisdictions / Legislation	IM / KM	Specialized Streams	FOI / Privacy Careers
1) Enhanced Mediation	1) Review of Significant Orders	1) PIA/TRA Interactive Session	1) Basic Access	1) Current Technology of Identity/ Surveillance (2 pts)	1) Anti-Terrorism Act; Privacy 4 years After 9/11	1) Security Classification	1) Police Network	1) Access & Privacy Careers
2) Tips on Preparing Representations	2) Legislative Labyrinth	2) Workplace & Off Premises Privacy Protection	2) Basic Privacy	2) Technologies to Verify Privacy Policy Enforcement & Compliance	2) PHIPA and Municipalities	2) IM in the OPS: a Status Report	2) Municipal Sector - DoR&RD / AD	2) Delivering Access & Privacy Training In-House
3) What to do When a Privacy Breach Occurs	3) Precedent Setting Orders & JRs	3) How to a Privacy Culture in Your Organization	3) Basic Processing	3) PIA Documentation for Architects (data flow modelling) [2 pts]	3) PHIPA; 1 year Later	3) Closed Circuit Television		3) Building the FOI Team
		4) Privacy Action Plan	4) Advanced Access					4) WSIB In-House Training Experiences
		5) How to Hire a Privacy Consultant						
		6) Imbedding Privacy into the Project Life Cycle						

About "Toolkit for Change" Access & Privacy Workshop 2005

Government faces increasingly complex privacy, access and information management challenges. Our responses range from reinforcing a privacy aware culture to supporting a culture of openness to implementing security classification schemes. The Workshop will help you to navigate today's changing environment by equipping you with relevant, effective tools for our continually evolving conditions.

If your work involves access, privacy, information technology, communications, policy, planning, records management or program design, join us for a great learning and networking opportunity.



Public Record Sections 14(1)(c), 27; 21(1)(c), 37

A public record is a collection of personal information to which the public has access and where the personal information was collected and maintained "specifically" for the purpose of making it available to the public.

Public records contain personal information so the public need to know must outweigh the personal privacy interests of personal information made available. Personal information can be maintained in public records for reasons including:

- Program administration and services, (e.g. elector lists, assessment roll).
- Promoting government accountability, by providing information relating to the issuance of licences, permits, government contracts, etc.
- Promoting informed choice and consumer protection, (e.g. land registry, assessment roll, personal property security registration, licenses, permits)
- To support the fair determination of rights.

Key Features of Public Records

1. The record is available to all members of the public, not a select group.
2. A fee may be charged if it is not so high that it is a bar to access.
3. The record may be created for another purpose but is publicly available.
4. Public records may have purposes other than access. For example, the land tax register supports administration of the property tax program, and its information can be accessed for business purposes.
4. Access to a public record may require additional information, such as details or identifiers the institution uses to retrieve the record. Limited cost or inconvenience does not mean that records are not publicly available.
5. Personal information in a public record may not be public in another context. Public court records may show criminal convictions but a record of the same convictions in a personnel or security file would not be public.
6. In rare instances, parts of a collection of personal information are maintained as a public record, and other parts are not publicly available.

How Public Records Are Created

In many jurisdictions, public records of personal information are created by statute or regulation. In Ontario, public records can be created either by:
a) Law; or
b) Policy decisions by institutions.

a) Law

Statutes, regulations or by-laws designating public records may contain terms and conditions for the administration of the information. Often, the authority to charge fees, times and location of access, are prescribed in legislation.

b) Policy Decisions by Institutions

An institution may by policy designate a record public if a "public need to know" outweighs personal privacy interests of information in the record.

Factors to Consider

Factors to consider in the creation and maintenance of public records include:

- What personal information will be affected?
- What privacy rights attach to the affected personal information?
- Does a public "need to know" outweigh relevant privacy interests?
- Will the release of the information foster informed choice?
- Will the information be accessible to everyone?
- Does the public need the information to assist in the conduct of business?
- Would the public availability of the information be an unjustified invasion of personal privacy?
- Is the personal information particularly sensitive?
- Is the information relevant to a fair determination of rights?

(Municipal) Freedom of Information and Protection of Privacy Act (M/FIPPA) sets out no public record rules so the need for disclosure must be balanced against privacy interests. A key factor is avoidance of disclosures of personal information that constitute an "unjustified invasion of personal privacy".

Access to Records That Contain the Requester's Personal Information

Individuals can be denied access to records containing their own personal information under the exemptions at s.49/38. By contrast, s.21/14 applies when the record does not contain the requester's personal information.

It is established practice to consider the applicability of s.49/38 to entire records rather than just the parts or aspects of the record that contain personal information, as is done under s.21/14.

Checklist

- Does the information qualify as personal information under s.2 of M/FIPPA?
- Was the information supplied by the requester? -- It is generally an absurd result not to disclose information it to its supplier
- Can the information of the third party be reasonably severed?
- Is disclosure of the third party information an unjustified invasion of privacy as per s.14(3)/21(3)?
- Despite considerations of s.14 (2), 14(3)/ 21(2), 21(3) -- Discretion can be exercised to release under S.38/49
- Should third parties be notified under s.21/28? -- Beware disclosure of requester personal information in the notice process
- Has the head clearly exercised their discretion to apply other exemptions?

Frivolous & Vexatious Requests
S4 FIPPA/S10 MFIPPA

The Act states that such a request must be part of a pattern of conduct:

1. that amounts to an abuse of the right of access, or
2. where responding to the request would interfere with the operations of the institution.

Or the request must have been made in bad faith or for a purpose other than to obtain access.

The following may guide you in determining whether a particular request would qualify as frivolous or vexatious:

A "pattern of conduct" requires recurring incidents of related or similar behaviour (or requests) on the part of the requester – or with which the requester is connected in a material way. The length of time over which behaviours occur is also a factor.

Examples of "abuse of process" include:
A volume of requests and/or appeals that would be considered excessive by reasonable standards, combined with other factors such as:

1. Nature and Scope of Request(s)
   a) Requests excessively broad, varied in scope, unusually detailed
   b) Requests identical to or similar to previously files ones, or that revisit previously addressed issues.
2. Timing of Request(s)
   a) Connected to court proceedings or some other extranious factor. (eg: more requests and appeals after institution sues individual).
3. Purpose of Request(s)
   a) Requests intended to accomplish some objective other than to gain access such as to attack the system and/or waste resources. (Purposes can sometimes be inferred from the requester's behaviour).
   b) Requests submitted without basis, for "nuisance" value, to harass.
   c) Is requester allied with other requester(s) whose aim is not Access?
4. Other Factors
   a) Institution conduct (eg. Contributing to problem through delay).
   b) Cumulative nature and effect of requester's behaviour.

"Bad faith" is not simply bad judgment or negligence. It requires conscious wrongdoing, a dishonest or malicious purpose. It requires an intention to use the access process for nuisance rather than to obtain information. Bad faith cannot merely be based on a history of disagreement or dislike between an institution and the appellant, nor that records may, after examination fall outside the ambit of the Act, nor that the appellant may have obtained access to some confidential information outside of the access process.

FOI Request Clarification

1. Discuss the request promptly with the program area. Assess the need for requester clarification. For large or complex requests, prepare options/alternatives for the requester.
2. Contact the requester quickly to clarify. This builds rapport and shows the requester your serious, professional approach and builds credibility.
3. Give the requester time to explain. Listen carefully and make complete notes.
4. Restate the clarification and come to an agreement with the requester.
5. Explain the request process, timelines, fees and possible outcomes to the requester.
6. Arrange conference calls with requester and capable program area staff to discuss complex requests – Do not become a go-between.
7. Document and confirm clarifications immediately in a letter to the requester.
8. When you can't call the requester, send a clarification/close-by letter, including the option of closing the file if the requester does not contact you by a specified, reasonable date.

Forwarding / Transferring A Request - S25/18

Forwarding

If an institution receives a request for a record that is not "in its custody" nor "under its control", the institution has an obligation under the M/FIPA to, within 15 days:

- determine if another institution has either custody or control of the record;
- if so, forward the request to that institution along with the application fee; and
- give the requester written notice of the forwarding.

It may not always be possible to forward an application fee, in which case the institution should ask the requester to submit a fee to the new institution.

Forwarding is possible to M/FIPPA institutions but not to bodies outside the acts, such as Federal Government or private entities.

Transferring

Institutions can transfer requests for records that they hold but in which another institution has a greater interest. An institution has a greater interest if:

- the record was originally produced in or for that institution; or
- the record was not originally produced in or for an institution, the other institution was the first institution to receive the record or a copy of it.

Requests can be transferred within 15 days of receipt. If forwarding is not possible.

For example, with Federal Government bodies, consultation is suggested. Time extension is permitted for consultations.

Transfer conditions in this provision are discretionary so institutions do not have to transfer requests, even when another institution has a greater interest in the record.

Shared Interest in a Request

When more than one institution has responsive records, the requester must be informed and provided with contact names and addresses in the other institutions' access offices.

Notice of Collection

When an institution collects personal information, either directly from an individual to whom the information relates or from another source, M/FIPPA requires that the individual must be informed that the collection has occured.

Section 39(2)/29(2) requires notices of collection to contain:

A - Legal authority for the collection

Legal authority for collection of personal information is usually established by statute or by-law. The notice should reference provision(s) that permit the collection. Where an act or by-law does not specifically authorize the collection, the notice should reference section(s) establishing the activity or program under which the information is collected.

B - Principal purpose(s) for which the personal information is intended to be used

C - Title, business address and telephone number of an official of the institution who can answer an individual's questions about the collection

Notices of collection are normally placed on government forms used to collect personal information when registering individuals for a service or a benefit.

Notice of collection requirements can also be satisfied by:

a) Posting a notice of collection where it will be clearly seen by individuals whose personal information is being collected,

b) Providing a verbal notice of collection at the point of collection.
- It is useful to verbal notices of collection for future verification.

September 2005

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6 Labour Day	7	8	9	10	11
12	13 PWG Meeting	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

October 2005

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6 Access & Privacy Workshop 2005 "Toolkit for Change"	7	8
9	10 Thanks-giving	11	12	13	14	15
16	17	18	19 PWG Meeting	20	21	22
23	24	25	26	27	28	29
30	31					

November 2005

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11 Remem-brance Day	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

December 2005

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15 Co-ordinator Meeting	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31