

*If you wanted to know...*

# ***Why Web sites need Privacy Policies***

***... Read on ...***

The rapid growth of the World Wide Web (Web) has led many organizations to launch or consider developing a Web site. Increasingly, one of the key issues that determines whether an individual will actually enter a site that he or she finds potentially interesting, or is willing to provide accurate information if required to fill in forms, is the site's privacy policy, or lack thereof.

As opinion polls consistently show, individuals are very concerned about how their personal information<sup>1</sup>, which many Web sites collect, will be used. One survey<sup>2</sup> found that approximately *80% of respondents were apprehensive about using the Internet (Net) because of privacy concerns*, while another<sup>3</sup> found that *roughly 95% were interested in seeing the privacy policies of Web sites*.

The Information and Privacy Commissioner/Ontario has developed a set of best practices for Web sites, offering practical suggestions on how to address the public's privacy concerns. These best practices incorporate the Canadian Standards Association's fair information practices.

## **First Step**

Displaying a privacy policy in a prominent place on the home page of your organization's Web site is the first best practice. This privacy policy should indicate:

- what personal information is being collected;
- why it is being collected;
- how it will be used;
- who will have access to it;
- how long you will retain it;
- how you will dispose of it;
- who in the organization to contact for more information about the policy.

The point of the privacy policy is to eliminate the uncertainty, for the online user, of what you may or may not be doing with the personal information you collect. *Excerpts of four privacy policies are attached.*

<sup>1</sup> "Personal information" is defined in the Act as "any recorded information about an identifiable individual."

<sup>2</sup> Business Week/Harris poll of March 16, 1998.

<sup>3</sup> 1997 Center for Democracy and Technology survey.





The minimum standard would be to post a short statement at the top of a page where users input personal information, with a message as basic as: “Privacy Notice: All information collected by XYZ Organization will be kept confidential within our organization and will only be used for completing your order.”

## Use of Personal Information

A key question to ask yourself when collecting personal information is, are you collecting only what is necessary to accomplish the purpose? Allowing users to “opt-out” of providing personal information, where that information is not completely necessary, reassures those users of your intentions. For example, you may need to collect names and addresses to complete an order, but it’s seldom really necessary that this information be included in a survey of customer satisfaction.

Allowing users to opt-out benefits the organization in three key ways. First, because users have given the information voluntarily, it is more likely to be accurate. Second, you will also be more likely to get people to actually provide data you are asking for, and to do so truthfully. Users that might not have completed the survey at all, will be more likely to complete it if they can opt-out of providing information that they do not wish to disclose. And finally, allowing users to opt-out of providing certain information increases your credibility.

## Disclosing Personal Information

Web site operators may wish to disclose client information via a Web site in certain cases, such as the status of orders or account balances. When personal information is available from your Web site, privacy-protective steps need to be taken. There are two key issues: One, you should use some form of verification technique to verify that requesters are, in fact, who they say they are. And

two, you should either use encryption technology to keep information sent over the Net secure, or warn the user that you do not use encryption technology and that any information sent will not be secure — which will allow the individual to make an informed decision about whether or not to proceed.

As you would verify the identity of a person over the telephone before disclosing information, the same care needs to be taken when disclosing information over your Web site. Avoid using items such as date-of-birth, telephone number or social insurance number as identifiers since these may be known by others.

## Impact of New Technology

Ultimately, through still-evolving, privacy-enhancing technology, individuals will be able to pre-set what information they are prepared to release to a Web site. The World Wide Web Consortium’s *Privacy Preferences Project* (P3P) focuses on developing standards that will allow for the comparison of an individual’s pre-set privacy conditions with a Web site’s privacy practices. If the criteria do not match, the visitor would be advised of this and can decide whether to negotiate with the site or leave.

## Disposing of Information

If, as a Web site operator, you eventually want to dispose of some of the personal information that you have collected, it should be done in a secure manner. Electronic records should be removed using a utility program that makes the data unrecoverable — simply deleting files does **not** do this. And if you have generated paper records from the information you have collected, they should be shredded or incinerated, not discarded in the regular garbage or recycling bin. *The Information and Privacy Commissioner/ Ontario has practical guidelines available on the secure disposal of personal information.*



## Pertinent Reminder

Most Web sites have links to other sites on the Net. On your home page or pages with such links, advise or remind your visitors that when they use such links, they are leaving your site for another, and your privacy policy no longer applies.

## Conclusion

If you're setting up or revising a Web site, consider establishing and posting your privacy policy in a prominent position. Net users will be looking for this because they want to know what information you're collecting and how you will be using it. If you want visitors to linger at your Web site, this is one of the best ways to ease surfers' concerns, get them in to see what you've got, and keep them coming back for more!



### *If you wanted to know...*

is published by the **Office of the Information and Privacy Commissioner.**

If you have any comments regarding this publication, wish to advise of a change of address, or be added to the mailing list, please contact:

**Communications Department**  
*Information and Privacy Commissioner/Ontario*  
80 Bloor Street West, Suite 1700  
Toronto, Ontario M5S 2V1  
Telephone: (416) 326-3333 • 1-800-387-0073  
Facsimile: (416) 325-9195  
TTY (Teletypewriter): (416) 325-7539  
Web site: <http://www.ipc.on.ca>



20% recycled  
paper,  
including 20%  
post-consumer  
fibre



## Appendix — Sample Privacy Policy Excerpts

Organizations develop Web sites for various purposes. For example, the IPC has a Web site established to give interested parties access to a variety of different information, including orders issued, papers published, and best practices in the access and privacy field. Other Web sites are established for other purposes, such as ordering products, electronic banking, or playing games. Therefore, an organization's privacy policy will vary according to the purpose of the Web site. Here are a selection of privacy policies from some well-known organizations.

### ***American Express***

(<http://www.americanexpress.com/corp/consumerinfo/privacy/privacystatement.shtml>)

Excerpt: When you browse any American Express Web site, you do so anonymously. Personal information — including your e-mail address — is not collected. Some of our Web sites, however, may request that you voluntarily supply us with personal information, including your e-mail address and account number (if you are an American Express Cardmember or InvestDirect user), for purposes such as correspondence, site registration, checking your bill or investments online, making a purchase, or participating in online surveys.

### ***Microsoft***

(<http://www.microsoft.com/info/privacy.htm>)

Excerpt: Although microsoft.com does not provide your e-mail address or phone number to third parties, we may carefully select other companies to send you information through postal mail about their products or services. If you do not want us to do this, you may opt out when you give us your Personal Information (by selecting the option stating that you do not wish to receive such marketing materials from third parties). Additionally, if you do not want microsoft.com to send you e-mail or postal mail regarding Microsoft products or services, you may opt out when you give us your Personal Information (by selecting the option stating that you do not wish to receive such marketing materials from Microsoft.com).

### ***Wired***

(<http://www.wired.com/home/digital/privacy/>)

Excerpt: Wired Digital Inc. ... believes that strong electronic privacy is crucial for the ongoing success of the Internet as a service, commercial, and entertainment medium. To this end, unless you designate otherwise, the information you enter here will be known to only two parties: you and Wired Digital Inc. We pledge that Wired Digital Inc. will not release your personal data to anyone else without your consent - period.

### ***The World Wide Web Consortium***

(<http://www.w3.org/Consortium/Legal/privacy-statement#Public>)

Excerpt: As is typical, we log http requests to our server. This means that we know the originating IP (e.g. 18.29.0.1) address of an agent requesting a URL. We do not log the the specific identity of visitors. We occasionally analyze the log files to determine which files are most requested and the previous site or user agent which prompted the request. Our logging is passive; we do not use technologies such as cookies to maintain any information on users.

Logged information is not disclosed outside of W3C host site personnel. Aggregate (completely non-identifying) statistics generated from these logs may be reported as part of research results. The logs are permanently archived as raw research material. We use member-related information for the purposes of administering the W3C, and communicating and collaborating with our members.

This statement ... does not apply to our non-member site nor e-mail sent to W3C staff or lists. Any questions regarding the Web site and the privacy policy can be directed to [site-policy@w3.org](mailto:site-policy@w3.org). E-mail interactions are guided by general net-etiquette conventions.

Members' interactions with the site are authenticated. Consequently we have the capability to identify users and their activities. 1.By requesting a password you are added to our newsletter mailing list and your identity is relayed to Advisory Committee representative (AC rep). 2.We trace membership of lists for chairmen of Working Groups....