

Fair Practices Document

- Introduction

Internet Service Providers have spoken repeatedly about self-regulation as a viable alternative to being regulated by the government. CAIP as a representative of Internet Service Providers has done so too. This Fair Practices Document is an effort to add substance to those words.

Fair Practices Policy Statement

- 1. CAIP Members will provide their products and services in a responsible manner, ensuring that the services that they provide to their customers meet the service levels promised.**

Policy

- 2. CAIP Members will communicate with their customers in a clear, accurate and comprehensible fashion.**

Policy

- 3. CAIP Members will make information about the benefits and the risks of Internet use available to their customers so that they can make informed choices about how they and their families or employees use the Internet.**

Policy

- 4. CAIP Members will not knowingly host illegal content or condone illegal conduct, and they will take action when notified about either.**

Policy

- 5. CAIP Members will not knowingly allow their services to be used for the transmission of unsolicited bulk e-mail, especially unsolicited commercial bulk e-mail between parties that have had no previous commercial relationship.**

Policy

- 6. CAIP Members will work to resolve any disputes with customers or members of the public in a manner that is fair, timely, effective and affordable.**

1.0 Fair Practices Policy Statement - Responsible Service

Policy Components

– Moving Toward Implementation

CAIP Members will provide their products and services in a responsible manner, ensuring that the services that they provide to their customers meet the service levels promised.

1.0 Each CAIP Member will institute and implement an Authorized Use Policy, and that Policy shall include instructions on how to contact an appropriate person within the organization when customers experience a problem.

Commentary: Setting an Authorized Use Policy is part of defining the relationship that an ISP will have with its customers and contributes to how an ISP will interact with its peers and the community

1.1 Each CAIP Member will make its Authorized Use Policy available to its customers and the public.

1.2 Each CAIP Member's Authorized Use Policy will be a living document, enforced, reviewed and updated on a regular basis.

2.0 At a minimum, CAIP Members will provide customer service in the following areas: (i) sales, (ii) technical, (iii) billing and (iv) complaints.

2.1 CAIP Members will clearly and accurately describe the methods that a consumer can use to contact them for service.

2.2 CAIP Members will provide consumers with some tools to solve their own problems.

2.3 CAIP Members will ensure that their representatives who deal with customers are trained in the area or areas for which they are responsible: sales, technical, billing and complaints. This responsibility exists even when all or part of their customer support functions are outsourced.

2.4 CAIP Members will establish procedures for responding to customer inquiries and complaints.

3.0 CAIP Members will provide a stable Internetwork for their customers.

- 3.1 When a CAIP Member chooses to specify a service level for one of its products, that service level must be supported with appropriate warranties in its contract.**
- 3.2 CAIP Members will maintain appropriate levels of general liability insurance.**
- 3.3 When it becomes necessary to close down a point of presence (POP), CAIP Members will first notify their affected customers so as to give them a commercially reasonable amount of time to secure service from an alternate provider.**

Commentary:The amount of time required will vary depending on the type of customers and the options available to them. If there are several different options available, it will not take residential customers long to find a new provider and notify their friends and family. It is a different story for business customers who have lines that may have to be rerouted, customers to be notified and stationery to reprint.

4.0 CAIP Members will provide a secure Internetwork for their customers.

Commentary:Although there are many similarities that exist between all Internet Service Providers, it does not mean that all Internet Service Providers are alike. Each will have different organizational needs that will affect its decisions with respect to security. All ISPs will have servers and other networking equipment, business information and customer information, but the amounts that a small, local ISP will have will differ greatly from those of a larger regional ISP or a still larger national ISP. Similarly, a large national ISP will have a higher profile than a local ISP, increasing the likelihood of individuals testing its security systems. Consequently, it is very important that each CAIP Member scrutinize its business and assess the risks to it.

- 4.1 CAIP Members shall assess their networks for risks on a regular basis. The assessment will identify: the Member's organizational needs, its assets, risks to those assets and the risks that the Member may pose to those to which it interconnects.**
- 4.2 Each Member will have and implement a Security Policy that is appropriate for its organization.**

5.0 CAIP Members will treat their peers with courtesy and act in good faith when dealing with them.

Commentary:The industry is as interconnected as the Internet, and consequently, depends on a certain amount of co-operation. Additionally, there are many issues where it is and will be necessary to work together as an industry. A certain amount of trust and respect is necessary.

5.1 CAIP Members will participate in industry activities and assist in establishing and maintaining the integrity of the industry.

2.0 Fair Practices Policy Statement - Communications

CAIP Members will communicate with customers in a clear, accurate and comprehensible fashion.

Policy Components – Moving Toward Implementation

1.0 CAIP Members will ensure that their contact information is readily available to customers including any contact information that is to be used for a specific purpose like customer service.

Commentary: Clear communications help to build strong relationships with customers. Each party knows what it can expect to receive and what it must give in return. Ambiguous or misleading communications create opportunities for misunderstanding and generally result in complaints. By reducing the possibility of a misunderstanding, CAIP Members can reduce the number of complaints with which they must deal. Consequently, CAIP Members should be able to improve their rate of customer retention. As well, their employees will be able to focus on running the business instead of fighting fires.

Lastly, if a customer can readily determine to whom they must speak in order to resolve a problem that they are experiencing, then they will not end up being frustrated by both the problem and the process of finding a solution.

2.0 CAIP Members will describe their products and services accurately.

Commentary: Although consumers are becoming increasingly Internet savvy, it is still not reasonable to assume that they will have the same expectations about what a service should include or how it will perform as someone who is knowledgeable about the Internet. The language should be plain, and definitions or explanations should be provided when technical terms are used.

3.0 CAIP Members will make their policies that affect customers available to their customers.

3.0 Fair Practices Policy Statement - Educating Customers

CAIP Members will make information about the benefits and risks of Internet use available to their customers so that they can make informed choices about how they and their families or employees use the Internet.

Policy Components

– Moving Toward Implementation

Commentary:As the Internet expands its reach to growing numbers of users, an increasing number will have little or no technical knowledge to use as a base for evaluating whether or not they should or should not do something on-line. This uncertainty may result in fears which could prevent them from taking advantage of all of the possibilities of the Internet. This uncertainty could also leave them vulnerable to Internet predators. With increased knowledge, a customer should be able to make the best of their time interacting with the Internet.

1.0 CAIP Members will make available information about the risks associated with Internet usage and about ways for customers to address these risks.

See following pages for Parent's Tip Sheet and Child's Pledge

CAIP's Childrens's Online Pledge

Post this by your computer!

1. **I will not give out information about myself or my family without getting permission from my parent or guardian.**

These are some of the things that I know not to tell:

- my name
- my telephone number
- the name of my school
- my parent's or guardian's name
- my brother's and sister's names
- my address
- my picture
- the name of any group or team that I belong to
- my parent's or guardian's address or telephone number at work

2. **I will not tell my password to anyone but my parent or guardian.**
3. **If I see something on-line that makes me uncomfortable or I receive an email that makes me uncomfortable, I will not respond, and I will tell my parents right away.**
4. **I will not open emails, links, URL or other files from people who I do not know and trust.**
5. **I will not arrange to meet anyone who I have met online without getting my parent's or guardian's permission, and if I get that permission, I know that a parent or guardian must approve the location and come with me.**
6. **I will not go online for more than _____ hours in a day and _____ hours in a week.**
7. **I will not intentionally look for sites that deal with:**

_____; and
_____.

8. **I will help my parent or guardian learn about the Internet.**

Signature: _____

Name: _____

Date: _____

CAIP's Internet Tips for Parents

- 1. Keep the computer in a common area within your home.**

Do not keep the computer in your child's bedroom: it is not an inanimate tool like a desk or an atlas. Keep the computer in the kitchen, den or family room or go with your child when they go to use the computers at the public library. This way you as a parent and any other adults in the house can check in on your child as he or she explores the Internet. If it isn't possible to keep the computer in a common area of the home, then it is even more important to check in on your child while they are on-line and to spend time with your child while they are online.
- 2. Spend time with your child, on-line.**

Just as you teach your child about the real world by exploring it with them, guide them through the on-line world. Learn about the services that your child uses by taking the time to see what they are doing on-line and where their interests lie. If you run into content that is offensive to you, talk to your child about it: explain why you believe the material is harmful and what you intend to do.
- 3. Report suspicious activity.**

Encourage your child to tell you when they run into content that they are unsure about, and not to respond to it. Upon reviewing the questionable material, if you believe that someone on-line is doing or about to do something illegal, then you should report it to the appropriate authorities. Make sure that you keep copies of all of the email messages including the header information. The authorities will need them.
- 4. Set reasonable rules and guidelines for your child, and decide whether or not to use blocking or filtering software.**

Discuss your rules and guidelines with your child, post them near the computer and monitor your child's compliance. The rules should set reasonable limits on the amount of time spent on-line. If you decide to use blocking software, then find one that is consistent with the rules and guidelines that you have set. Additionally, you should take the time to learn the strengths and limitations of the package that you choose. Even the best programs are not a substitute for an involved parent.

Cyber Patrol <http://www.cyberpatrol.com>
Net Nanny <http://www.netnanny.com/>
- 5. Monitor your credit card bill and your phone bill.**

A credit card number is required to gain access to many adult Internet sites, and a modem can be used to dial phone numbers other than the phone number of your Internet Service Provider.

6. Tell your child not to give out personal information on-line.

This is Internet version of “never talk to strangers”. Teach your child to never give out their name, address, phone number, school name or any personal information especially in public places like chat rooms and bulletin boards.

Using a nickname or a pseudonym is common practice on the Internet, and it is a way in which your child can protect their personal information to a certain extent.

7. Know your children’s on-line friends.

It is possible to form beneficial and lasting relationships on-line, but there are people who misrepresent themselves on-line and there are people who will take advantage of your child. Make sure that your child knows not to arrange to meet their on-line friends without your permission. If you permit a meeting with an on-line friend, then make sure that: (i) you accompany your child and (ii) they meet in a public spot.

8. Learn more about the Internet.

Take the time to learn more about the Internet. Ask your child to teach you what they know. Look for courses being offered in your community. Surf on your own.

<http://www.media-awareness.ca>

<http://www.safekids.com/>

<http://www.safeteens.com/>

<http://www.safekids.com/computers.htm>

4.0 Fair Practices Policy Statement - Illegal Content and Conduct

CAIP Members will not knowingly host illegal content or condone illegal conduct, and they will take action when notified about either.

Commentary:This policy statement is deceptively simple. It assumes that the answer to the question of whether or not a specific image, text or act is legal or not is obvious or available. Realistically, the answer to that question is seldom obvious. The notion of “I know it when I see it” does not necessarily align with the Criminal Code or other laws. As well, the time required to reach a judicial determination is too long to keep a customer with a complaint on hold. Consequently, it is important that CAIP Members develop an approach to content issues that takes into account the applicable laws, the member’s particular circumstances and beliefs which can be applied consistently. Still, it is important to remember that behavior that would be considered illegal in the actual world such as uttering death threats remains illegal even when the method used to carry out the behavior in question involves the Internet.

Policy Components – Moving Toward Implementation

- 1.0 CAIP Members will ensure that their customers can find the contact information that they need when they want to make a complaint about content or conduct on the Internet.**
- 2.0 CAIP Members will have procedures in place for handling complaints with respect to content or conduct.**

Commentary:A procedure for handling this type of complaint will be very similar to the ISP’s procedure for handling complaints with respect to other types of content, but there will be at least one or two additional complications. Law enforcement officials will be involved. The identity of the user behind the behavior or the content will likely be much more of an issue, so privacy issues will come into play, as well. In the instance of a crime that may be committed, time will be of the essence.

- 3.0 CAIP Members will advise customers with questions regarding the legality of specified content or conduct to obtain independent legal advice.**
- 4.0 CAIP Members will cooperate where possible with government officials, international organizations and law enforcement authorities.**

5.0 Fair Practices Policy Statement - Prohibiting Unsolicited Commercial E-mail

CAIP Members will not knowingly allow their services to be used for the transmission of unsolicited bulk e-mail especially unsolicited commercial bulk e-mail between parties that have had no previous commercial relationship.

Commentary: Typically, bulk e-mails of a non-commercial nature are included in the definition of spam (chain letters, virus hoaxes, assorted urban legends). Non-commercial bulk e-mails are not being included in the definition of spam for this document because the approach for dealing with these types of e-mails is less complex than dealing with unsolicited commercial e-mail. Since monetary interests are not involved, ISP authorized use policies and education should go much further in dealing with these types of bulk mailings.

It should be noted that only the spammers who flood the Internet with unsolicited commercial e-mails can resolve this problem on their own. ISPs, Internet users and governments can put social, technical and legal obstacles in the way of these bulk e-mailers, but the bulk e-mailers will find ways around them so long as they believe that they are benefiting commercially from their use of unsolicited commercial e-mail. Consequently, this document does not propose a solution to the problem at hand. Instead, it focuses on helping CAIP Members make responsible choices. Additionally, its companion document “SPAM – User Tips” focuses on educating individuals so that they can minimize the impact of unsolicited commercial e-mail on themselves.

Policy Components – Moving Toward Implementation

1.0 Each CAIP Member’s Authorized Use Policy will prohibit: (i) sending unsolicited bulk e-mail and (ii) mail bombing.

1.1 Each CAIP Member’s complaints procedure will deal with complaints about unsolicited commercial e-mail.

2.0 Each CAIP Member will make information available to its customers about how to reduce the amount of unsolicited commercial e-mail that they receive.

Commentary: There is no possible way that would allow an Internet Service Provider to continue to operate and eliminate spam from its customers' mailboxes. Consequently, any approach taken must be taken jointly between the Internet Service Provider and its customers.

See following pages for CAIP's Tip sheet on Dealing with Unsolicited Bulk E-mail

CAIP's Tip Sheet on Dealing with Unsolicited Bulk Email

1. If you want to avoid junk emails altogether, then the only realistic solution that you have is to not use the Internet – never browse the web, never purchase anything over the Internet, do not subscribe to any mailing lists, never post to Usenet and do not give your email address to anyone.

Commentary: Some spam is pretty much inevitable. For most users, the goal should be to minimize the amount that you receive.

2. Using two different email accounts is one way of managing spam. Reserve one email address for your friends and family, another for your business associates and a third when you are browsing or posting to news groups.

Commentary: This does not mean sign up for three accounts (unless you actually need that many hours of service). Many ISPs already offer multiple mailboxes in some of their service plans. Check to see if your ISP provides these services.

3. When you are on-line, guard your personal information.

Commentary: Just because a web site asks for your personal information does not mean that you need to give it to them. Certainly, do not give it to them without checking their privacy policy.

- 3.1 Reconfigure your browser.

Commentary: As a default, many browsers are set to reveal certain information about their user. Start your browser, and using the help function look for information under the following headings: Personal Profile, Security and Privacy. The help function should provide you with the information that you need to make appropriate changes. This information may also be available on your Internet Service Provider's web site.

- 3.2 Change the reply-to setting on your email program when you are posting to news groups.

Commentary: If you still want people who actually read the postings in the newsgroup to be able to reply to you, then you may want to adopt this common practice:

- a. **Insert an obvious word into your reply address. For example, if your address is**

“whyme@isp.ca”, your reply address might be “whyme@isNOSPAMp.ca”.

- b. In your signature file, instruct any one who wishes to send email to you to delete, “NOSPAM”, from your return address.

- 3.3 Do not register with a “DO NOT SEND” list.

Commentary:These lists rely on the co-operation of spammers, and there really is no incentive for any given spammer to stop sending email to the addresses that these sites supply to them. The incentive is even lower when you consider that these are lists of valid email addresses.

4. Do not send email to a spammer.

- 4.1 Do not email back to the spammer asking them to remove your name.

Commentary:It is not uncommon for spammers to include a return email address in their spam for the sake of removing your name from their list. Unfortunately, for those bulk emailers who actually do honor requests to remove names from their lists, most spammers do not honor these requests. Instead, they regard them as proof that the address is active, making it a more desirable target.

- 4.2 Do not reply to spam.

Commentary:Most likely, the “reply to” address is invalid. If the address is not invalid, then there is a good chance that it is not the spammer’s address.

- 4.2.1 Do not try to disrupt the spammer’s email by sending large quantities of mail to the reply address or by sending an exceedingly large email.

Commentary:If the address is invalid, you have successfully disrupted your own email account as the notice or notices of failed delivery appear. If the address is valid, then you have probably disrupted the email service of an innocent third party. Most likely, you have violated your ISP’s Acceptable Use Policy, and your email account is now in jeopardy. Responses like yours are almost as big a problem as spam.

5. Do contact the spammer's ISP.

Commentary:Unless the spammer has set up as their own Internet Service Provider, then they have probably violated the Authorized Use Policy of their Internet Service Provider.

Most Internet Service Providers will be responsive to your complaints. Spam is a problem for them too. It can slow down or shut down their service. It generates complaints from their peers and from their customers. It may even put their connection to the Internet at risk if their upstream provider made them sign a contract that prohibited spamming.

6. Do contact your ISP. Find out what they are doing with respect to spam.

Commentary: Filtering at the ISP level may cause problems for you or those who wish to contact you for legitimate purposes. It is important to choose an Internet Service Provider whose approach to dealing with spam is consistent with your needs.

7. Do stay informed.

Commentary:There are countless web sites devoted to the elimination of spam. To find a wide sampling just use your web browser to search on "spam", "junk email", "unsolicited commercial email" and on "unsolicited bulk email".

Also, check out your own Internet Service Provider's web site for information on spamming.

8. If you are sufficiently outraged and have the resources, then taking legal action may be a possibility.

Commentary:Realistically, this is not an option for most users, but it probably is worthwhile to check to see if your Internet Service Provider is pursuing legal recourse against any spammers.

6.0 Fair Practices Policy Statement - Dispute Resolution

CAIP Members will work to resolve any disputes with customers or members of the public in a manner that is fair, timely, effective and affordable.