[Insert your organization's name here]

December 2006

COMPUTER NETWORK AND INTERNET ACCESS POLICY

Purpose and Permitted Use

_____ computer network is a work tool and is to be used by employees for legitimate work-related purposes. All such use is to be lawful and consistent with the agency's general reputation, standards and other workplace conduct rules. Internet use must be work-related and offensive sites and material must be avoided.

Incidental personal use of the computer network and Internet is permitted during break periods, provided such use is minimal, does not interfere in any way with the performance of your duties, and does not otherwise violate this policy.

The conduct of employees on the internet even outside of working hours may sometimes reflect on _____ Employees must therefore be prudent in their online behaviour at all times. This policy sets out guidelines for employees' use of social networking and blogging websites which must be followed even outside of working hours.

Prohibited Use

Things such as games, animated screen savers, humorously altered digital photographs or short digital movies can take up a great deal of valuable storage space on our network. They may also contain a virus or viruses, may be incompatible with our operating system or other programs, or may cause other difficulties with our network. At the very least, these things slow down our system. At worst, they can cause the network to crash, resulting in stress, frustration and lost work time. For these reasons, there are certain uses of our computer network which are not permitted.

_____ computer network will not be used for:

- any illegal, unethical or immoral purposes;
- sending, storing or transmitting offensive, objectionable, abusive, pornographic, obscene, sexist, racist, harassing or provocative messages, images or other materials, including adult-oriented web sites or news groups;
- defamatory, derogatory or false messages;

- running of a personal business;
- participation in on-line games or any non-work related chat groups;
- any use which compromises system integrity or which could degrade system performance;
- unsecured or unauthorized disclosure of confidential or privileged information;
- downloading material from the Internet including software, shareware, pornography, games, screen savers, digital photographs and digital movies. Storage of any of these items on the network hard drive or on your workstation hard drive is also prohibited;

Monitoring

The computer network, which includes all hardware, as well as all software, data, files and e-mail which resides on it, is owned by _____. The agency reserves the right in its sole discretion and without further notice, to intercept, retrieve, access, review, archive, destroy and/or disclose to others (including law enforcement authorities and courts) all computer network data and uses.

Users should have no expectation of complete privacy in anything they create, store, send or receive using _____ computer network. Use of the computer network constitutes an irrevocable consent to the monitoring and disclosure of system use and data and an agreement to comply with all other aspects of the computer network policy. In certain circumstances, the agency may access and disclose messages sent over its e-mail, Internet or computer system. These circumstances include but are not limited to:

- Regular maintenance of the computer network
- When the agency has a work-related need to access the employee's mailbox (e.g. if the employee is absent)
- When the agency has a need to access particular documents
- When the agency has reason to believe that the computer network is being used in violation of this policy

Passwords

Passwords are used for security but do not prevent management and/or information systems personnel from authorized monitoring and disclosure of system use and data.

Users are responsible for any and all activity which takes place using their user ID and password. Users should not use another person's user ID and password, nor should they give their user ID and password to another person, unless agreed to by both parties and with the knowledge and consent of the Director of Finance (who has oversight responsibility for information/Internet technology at _____).

As a security measure, passwords will be changed periodically. When this occurs, new passwords will be provided to you by our tech support firm.

Confidentiality

Users will not reveal in external e-mail transmissions personal information, including for example, photographs, home addresses or home phone numbers of clients or co-workers, unless granted permission to do so.

Unless expressly authorized to do so, users are prohibited from sending, transmitting or otherwise distributing proprietary or confidential information about _____.

As discussed below, these restrictions apply even when employees are using their own computers during non-work hours.

Security of Computer Resources

Unless expressly authorized to do so, users must never download files from the Internet or other on-line services, or use disks from non-_____ sources, without first having the material scanned with the agency's approved virus-checking software.

No software or programs of any sort are to be installed on a computer without the prior approval of the Director of Finance.

Recognizing that the network and storage capacities have finite limits, users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others.

Users must ensure that a general cleanup is performed, on a regular basis, of all documents and e-mails which are no longer required or which can be stored separately.

In order to protect our corporate information and data, users must store all files on the server drives (which are backed up nightly), and not users' C drives.

Social Networking and Blogging

Even where employees access social networking, blogging or similar websites from their own personal computers outside of working hours, they are expected to consider whether their actions might impact _____. Employees must be cautious where there is a risk that their actions on the Internet will harm the reputation or business of _____.

This means that employees must not make disparaging, threatening, defamatory or abusive comments about _____, about other employees, or about clients and/or children of clients on the Internet. Similarly, employees must not make comments that are reasonably likely to cause offence in relation to any of the prohibited grounds of discrimination set out in the Ontario *Human Rights Code*, including for example, race, gender, sexual orientation or national or ethnic origin.

A failure to respect this requirement may expose _____ to legal liability, either for defamation or for a breach of the *Human Rights Code*. Comments like these from employees could also seriously harm the reputation of _____.

Employees must also remember that they are required to respect the confidentiality of information they receive in performing their jobs. This means that employees must not disclose in online comments information which might identify clients, or information like addresses, phone numbers, photographs or other personal information about clients.

Employees should take care to maintain distance and professionalism with clients at all times. Employees should be cautious about making or accepting contact with clients online, and should be aware that any contact with clients carries risk as detailed above. If employees have clients as “friends” or contacts on Facebook or other social networking sites, they must be careful to maintain a very high degree of professionalism in all of their conduct on those sites.

Violations of Policy

Employees who contravene any part of this policy will be subject to disciplinary action, up to and including possible immediate termination of employment.