



## **POLICY AND PROCEDURE MANUAL**

### **POLICY 10 – INFORMATION TECHNOLOGY & SECURITY**

#### **Policy Intent**

The Humber Students' Federation (HSF) has taken extended efforts to provide a quick and reliable method of connecting HSF affiliates (full-time staff, part-time staff, club members, Directors, and HSF consultants or advisors) to the Internet. As an organization in a learning environment, the HSF recognizes the important role technology has in enhancing our business productivity. This policy will provide guidelines governing the appropriate use of the HSF information technology infrastructure for Internet functions. The equipment used for providing high quality Internet access represents a considerable investment and every effort must be taken to ensure the long-term integrity of the information technology infrastructure.

#### **Internet Usage Philosophy**

HSF affiliates are expected to use Internet access primarily for business-related purposes. This includes such functions as communicating with customers and suppliers, to research topics of interest, and to obtain useful business information.

HSF affiliates must conduct themselves honestly and appropriately on the Internet, respecting the laws of copyright infringement, software licensing, property rights, and privacy. All existing HSF policies (please see the HSF Policy and Procedure Manual) apply to an affiliates' conduct on the Internet. HSF affiliates must also consider issues of intellectual property, misuse of HSF resources, sexual harassment, data security, and confidentiality when using information technology infrastructure.

All unnecessary, or unauthorized, Internet usage causes server and network congestion. This slows other users' Internet access, detracts from work time productivity, consumes resources, and restricts equal access to printers and other shared devices. Unlawful, or unethical, Internet usage may also generate legal proceedings or draw negative publicity for the HSF.

The vast reach of the Internet allows each HSF affiliate an immense opportunity to broadcast the services and business operations of the HSF. With such a powerful communication tool, special care must be taken to maintain the clarity, consistency, and integrity of the HSF's corporate philosophy and image. Anything an HSF affiliate writes in the course of utilizing the Internet could be interpreted as representing the opinions of the HSF. Since such a potential for

misinterpretation exists, HSF affiliates are expected to be extremely mindful of their activities when using corporate resources to access the Internet.

While a high quality Internet connection offers a broad range of potential benefits, it can also present some significant risks to HSF data and information technology infrastructure should security guidelines not be followed. The following guidelines will illustrate the diverse range of complications that arise with information technology infrastructure. The predominating factor when governing information technology infrastructure is that network security is to be the first concern of all HSF affiliates. It is important to note that as an independent corporation, the HSF can be held accountable for any breaches of security, or confidentiality, that its affiliates participate in. These guidelines are in place to protect the organization, its affiliates, and the system resources from ill effects.

## **Policy Definitions**

**IT** - refers to information technology.

**Humber Students' Federation** (HSF) - includes all HSF affiliates, subsidiaries, and branches.

**Users** or **HSF affiliates** - refers to all employees (full and part-time), Directors, club members, and all other HSF advisors or consultants.

**Document** - refers to any kind of file that can be read on a computer screen as if it were a printed page. These include, but are not limited to: HTML files, files meant to be accessed by a word processing or desktop publishing program, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools.

**Graphics** - refers to all photographs, pictures, animations, movies, or drawings.

**Display** - refers to all monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions, and virtual-reality devices.

## **Detailed Policy Guidelines**

### ***Internet Usage***

The HSF has software and systems in place that monitor and record all Internet usage. Our security systems are capable of recording each World Wide Web site visit, chat, newsgroup, e-mail message, or file transfer into and out of our internal networks by any individual user. The management of the HSF reserves the right to do so at any time. No user should have any expectation of privacy when using the HSF corporate IT infrastructure for Internet usage.

### **Guidelines:**

1. At the request of the Executive Director or President, the Network Administrator will produce an Internet Activity Report each month. The Executive Director and President will review Internet activity and analyze usage patterns. The Executive Director and President will address any incidences of inappropriate activity conducted by employees. The Executive Director and President would also address any inappropriate Internet activity by directors. In cases involving directors, the HSF Board of Directors may be duly informed.
2. The Network Administrator, Executive Director, and President reserves the right to inspect any and all files stored in private areas of the HSF network in order to assure compliance with this policy.
3. The display of any kind of sexually explicit image, or document, on any HSF system is a violation of this policy. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded using the HSF network or computing resources.
4. The HSF uses independently supplied software and data to identify sexually explicit, racist, or hate Internet sites. The Network Administrator may block access to these sites. Users who accidentally discover that they can connect to these sites, or other potentially offensive material, must immediately disconnect from these sites and inform the Executive Director/Business Manager via email of such an occurrence. The ability to mistakenly connect to these sites does not constitute permission to do so.
5. The HSF's Internet facilities and computing resources must not be used to violate the laws and regulations of Canada, or any other nation, or the laws and regulations of any state, city, province, or other local jurisdiction in any material way. The use of any HSF resources for illegal activity is grounds for immediate dismissal and every effort will be made by the corporation to cooperate with law enforcement investigations pertaining to such activities.
6. Any software, or files, downloaded via the Internet onto the HSF network become the property of the HSF. Any such software, or files, may only be used in ways that are consistent with their licenses or copyrights.
7. No user may utilize HSF facilities to download or distribute pirated software or data.
8. No user may utilize the HSF's Internet facilities to propagate any virus, worm, Trojan horse, or trapdoor program code.
9. No user may use the HSF's Internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user, either internally or externally.
10. Any user of the HSF Internet facilities shall identify themselves honestly, accurately, and completely when participating in chats, newsgroups, or when setting up accounts on outside computer systems.

11. Only those employees or officials who are authorized to speak to the media, analysts, or at public gatherings on behalf of the HSF may speak or write in the name of the HSF to any newsgroup or chat room. Other users may participate in newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking for themselves only, not representing the opinions of the HSF. Where an individual participant is identified as an employee or agent of this HSF, the employee must refrain from any political advocacy and must refrain from the unauthorized endorsement, or appearance of endorsement, by the HSF of any commercial product or service not sold or serviced by the HSF, its subsidiaries, or its affiliates.

12. The HSF retains the copyright to any material posted to any forum, newsgroup, chat, or World Wide Web page by any user in the course of their duties.

13. Users are reminded that chats and newsgroups are public forums where it is inappropriate to reveal confidential HSF information, customer data, trade secrets, and any other material covered by existing HSF policies and procedures. Users releasing such confidential information via a newsgroup or chat, whether or not the release of such information is inadvertent, will be subject to the penalties provided in the HSF Policy and Procedure Manual.

14. The use of HSF Internet facilities to commit infractions, such as misuse of HSF assets or resources, sexual harassment, unauthorized public speaking and misappropriation of intellectual property, are prohibited as specified in the HSF Policy and Procedure Manual.

15. Because a wide variety of materials may be considered offensive by colleagues, customers, or suppliers, extreme caution should be taken in all incidence of storing, viewing, printing, or redistributing any document or graphic file that is not directly related to the user's job or the HSF's business activities.

16. Users with Internet access must take particular care to understand the copyright, trademark, libel, slander, and public speech control laws of all countries in which the HSF maintains a business presence. This is integral so that our use of the Internet does not inadvertently violate any laws that might be enforceable against the HSF.

17. Users with Internet access may download software for direct business use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license. The Network Administrator, under advisement with the Executive Director/Business Manager, may remove any software not licensed to HSF without due notice to the user.

18. Users should not use HSF Internet facilities to download entertainment software, games, or to play games against opponents over the Internet during regularly observed office hours.

19. Users may not upload any software licensed to the HSF, or data owned by the HSF, without the expressed authorization of the HSF affiliate responsible for the software or data.

## ***Technical Aspects***

1. User Identifications (IDs) and passwords help maintain individual accountability for Internet resource usage. Any user who obtains an ID or password for an Internet resource from the HSF must keep that password confidential. This HSF policy prohibits the sharing of user IDs, or passwords, obtained for access to Internet resources.
2. Users should schedule communications-intensive operations (such as large file transfers, video download, mass e-mailings, etc.) during lower network usage periods to optimize the networks reliability and performance during high network usage periods.
3. Any file that is downloaded from the Internet must be scanned for viruses before it is run or accessed.

## ***Security Aspects***

1. The HSF may install an Internet firewall to ensure the safety and security of the HSF's networks. Any user who attempts to disable, defeat, or circumvent any security facility will be subject to immediate disciplinary action which may range from suspension of Internet privileges to dismissal.
2. Files containing sensitive HSF data that are transferred in any way across the Internet must be appropriately encrypted.

## ***Work Station Capabilities***

All HSF systems and workstations must have the capability to operate the following minimum software applications: Windows Professional 2000, Microsoft Office 2000, Adobe Acrobat, Internet Explorer, and Microsoft Outlook 2000.

All users will have the ability to a printing device. Each Executive and full-time employee will have a business email address, access to a shared staff drive, rights to a personal home drive, and limited accessibility rights to the network system.

## ***Laptop Computers***

All of the above stated guidelines are also applicable to the use of laptop computers. One laptop computer shall be available at each campus for HSF business purposes only. The Executive and full-time employees are entitled to borrow the laptop for a maximum of 24 consecutive hours. The Executive Director/Business Manager must approve the use of laptops for extended periods, such as conferences.

The Executive Director at North campus and Office Manager at Lakeshore campus are responsible for monitoring the proper usage of laptop computers (sign-in and sign-out procedures, scheduled maintenance, etc.).



## ***Acknowledgment***

I acknowledge that I have received a copy of Policy 10 – Information Technology and Internet Security for the Humber Students’ Federation. I have read the document and understand the terms of this policy and agree to abide by them.

I realize that the Humber Students’ Federation’s security software may record and store, for management’s observation, the use of electronic e-mail messages I send and receive, the Internet address of any site that I visit, and any network activity in which I transmit or receive any kind of file. I understand that any violation of this policy may result in immediate disciplinary action, ranging from suspension of Internet access to dismissal from employment. In extreme instances, criminal prosecution may be warranted.

---

Signature

---

Name (Printed)

---

Date