

## Bora Laskin Law Library Agreement for Computer Support

Bora Laskin Law Library offers limited computer support only on the following conditions, which you are required to read and agree to.

Your full name: (please print)	Your email address:
Circle your status at the law school: <u>1st year</u> <u>2nd year</u> <u>3rd year</u> <u>Combined Program</u> <u>LL.M.</u> <u>S.J.D.</u>	

In this Agreement, the terms “we”, “us” or “our” refer to and include the University of Toronto, the Faculty of Law, the Bora Laskin Law Library and their employees, agents, successors and assigns. The terms “you” or “your” refer to you and your agents, heirs and representatives.

- 1) You represent and warrant that the statements below about your computer are true. If they are not true, your computer and the data and programs on it will be at great risk if the computer accesses a network or the Internet. If any of these statements are not true, you accept such risk.
  - a) You are a student currently enrolled at the Faculty of Law, University of Toronto. The computer you have asked us to help you with (“your computer”) is yours alone or you have all necessary authority to make the representations, acknowledgements and requests provided for herein.
  - b) You represent that, to the best of your knowledge,
    - (i) **Infections:** Your computer is free from software, installed with or without your knowledge, which could cause damage to another computer including viruses, worms, Trojan horses, and any and all other like software routines (“Infections”).
    - (ii) **Software patches:** You have updated the operating system, Internet browser and electronic mail program on your computer with all available software patches.
    - (iii) **Norton:** You have installed on your computer the Norton anti-virus software (“Norton”) available for free to U of T students at <http://antivirus.utoronto.ca> and have updated Norton within the last 24 hours.
    - (iv) **Backups:** All important data on your computer is backed up. You accept the risk of loss of any and all data and software which may be on your computer now.
    - (v) **Warranties/Service contracts:** Your computer is covered by an existing warranty or extended service contract.
- 2) You acknowledge that:
  - a) You are requesting us to provide certain limited computer support services for which you will not be charged a fee. These services may include but are not limited to: laptop configuration for the wireless network (including any necessary software installation), support for ExamSoft configuration and general computer troubleshooting.
  - b) We are not experts in computer maintenance or support and are only required to exercise ordinary care in providing you with computer support.
  - c) We have given you the attached document called “Best Practices for Protecting your Computer” and you are aware that more detailed information on protecting yourself and your computer is available for free online at UTOR-Protect at: <http://cns.utoronto.ca/UTORprotect/>.

- d) There is a risk if we are assisting you to configure your computer for access to any wireless network, including the University of Toronto wireless network (“UTORcwn”) that if you have not properly updated your operating system with software patches or installed Norton anti-virus software and kept your copy of Norton anti-virus software entirely up to date your computer may be infected with a virus that might damage your computer or result in the loss of some or all of the data on your computer.
- e) We only support the following wireless cards for use on UTORcwn (the “supported cards”):
  - 1. Enterasys RoamAbout (128 bit encryption)
  - 2. Dell TrueMobile (128 bit encryption)
  - 3. Airport wireless card for the Mac.

If you are not using a supported card: (i) It likely will not work on UTORcwn; and (ii) we reserve the right to refuse to even try to help to make an unsupported card work on UTORcwn.

- 3) In return for us providing you computer support at no charge, you agree that:
  - a) You will remain with your computer at all times while we are providing computer support and will be responsible for its safekeeping.
  - b) You release us and hold us harmless from any claims you might have for any damages caused by us to your computer arising out of our computer support, including, but not limited to, hardware failures, infections, incremental maintenance and support costs incurred, loss of use of the computer, loss of productivity, loss of profits and loss of data. For greater certainty, no financial damages or other remedy shall be available for any loss described herein or occasioned by our computer support, and no punitive and exemplary damages may be recovered hereunder.
  - c) This Agreement for Computer Support will apply to all future computer support we may provide you. However, from time to time we, in our sole discretion, might decide to amend this agreement, or to require additional or different legal agreements as a condition to obtaining further computer support, and you acknowledge that it shall be a precondition of the receipt of such support that you execute such amended, different or additional agreements.

If you agree to these terms and conditions and would like us to provide you computer support at no charge, please sign and date below.

\_\_\_\_\_  
Your signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
On behalf of the Bora Laskin Law Library

\_\_\_\_\_  
Date

## Best Practices for Protecting your Computer<sup>1</sup>

1. Install a copy of the Symantec® Norton AntiVirus (NAV) software on your computer(s) and make sure that the software is always up to date by running LiveUpdate on a daily-basis. Also, make sure that your anti-virus software is always running, is set for 'real-time' protection and that it is set up to automatically start up when the computer is rebooted. The NAV software is free to all faculty, staff and all students enrolled in degree-granting programs of the University for both on- and off-campus computers and is available for download at: <http://www.antivirus.utoronto.ca>.
2. Use a personal Internet firewall on your computer(s). This is a piece of software or hardware that filters what kind of network traffic can get to your computer. Deny all traffic by default and only enable those services that are needed. Windows XP has a built-in firewall. Check the following website for instructions on how to turn it on <http://www.microsoft.com/security/protect> ). ZoneAlarm from Zone Labs is a free firewall that is highly regarded (<http://www.zonelabs.com> ) Symantec also has personal firewall software (not free).
3. Keep your version of MS Windows (9X/ME/2000/XP) current with the latest updates and patches available from Microsoft. Whenever a vulnerability in Windows is discovered Microsoft will have a patch available on their website (usually at: <http://www.microsoft.com/security> ). When alerted, download the patch and install it as soon as possible. You can also setup Windows to automatically download and install updates on your computer. This feature is described on the Microsoft website at: <http://www.microsoft.com/security/protect>.
4. Back up important files regularly. Store backup media in a safe and secure place that is not susceptible to extremes of temperature, humidity, etc., preferably at a different location from your computer. CD-Rs are a good and cheap medium for data backup from a personal computer.
5. Use spyware/adware detection software. Spyware or adware is software that tracks your Internet surfing habits and can be malicious. It is often not recognized by anti-virus software. Spybot S&D (<http://www.safer-networking.org/> ) is free software that can find and remove spyware from your computer. It can also immunize your computer against further spyware installations. As with other protection software check for updates regularly.
6. Before clicking on any e-mail attachment, make sure that the attachment is something you were expecting – do not blindly click on any attachment. Scan for viruses before opening the attachments even if you know the source.
7. Before using media given to you by someone else, scan it for virus infections. Viruses can be transmitted on all readable media including diskettes, CDs, USB memory cards, and other types of memory media such as SmartMedia or Compact Flash.
8. Control the downloading of 'cookies' to your computer. A cookie is a small text file that is set by a web site and stored on your hard drive and can track your surfing habits. Set your Internet browser to "prompt" you whenever a cookie is about to be downloaded to your computer then disallow any cookies from websites that you don't want to have access to your computer. Cookies are used by many websites, such as the Law School's eCommunity, to control access so don't set your browser to block 'all' cookies or you may be locked out of some important websites.

---

<sup>1</sup> For a detailed explanation of "best practices" see the PDF document available online for free from UTORprotect website at the University of Toronto's Computing and Networking Services website at [http://cns.utoronto.ca/UTORprotect/best\\_practices.htm/](http://cns.utoronto.ca/UTORprotect/best_practices.htm/).