



ICMS Personal Computer Policy

February 2010

Scope

This document is intended to assist Students and Staff with the usage of personal computers and web-capable equipment such as PDAs, SmartPhones etc.

Access

IS PERMITTED TO THE WIRELESS (ICMS-Student) NETWORK

IS NOT PERMITTED TO THE WIRED NETWORK(using network cables).

Personal equipment is not permitted at any times on the ICMS or Touraust cabled network. It is prohibited to connect a personal device to the Ethernet LAN in a classroom, study area or office. All connections to the cabled network are logged and it is a violation of the terms of your contract or enrollment to connect a personal device.

Access is permitted to the ICMS-Student wireless network with the understanding that all users must adhere to the ICMS Acceptable use policy. Excerpts of the policy are available in this document. For full listing of the policies, please see the ICMS Acceptable Use Policy

Network Security

As personal Laptops and Desktops are not college property, ICMS is under no obligation to ensure the integrity of said devices. ICMS will also take no responsibility for attacks by malicious users when connected to the wireless network. However, as a company, ICMS want to assist students and staff wherever possible and therefore have the following recommendations that should minimize the risk of attack. Also, please do not assume that because you run a certain operating system (Mac OSX, Linux, Unix, Windows) that you are immune to attacks, exploits or virii. All it takes is a single vulnerability and your PC can but host to a botnet.

Firewall

Students are recommended to use a firewall at all times. Student computers connect to the internet directly and are subject to malicious attacks. Regardless of operating system installed, use a firewall at all times. Please contact the IT Department for assistance in selecting or installing a firewall. As this is for a personal computer, support is provided on a best effort basis.

Anti-Virus

Students are also recommended to use an Anti-Virus product at all times. The best products are typically available from large companies and are not free. However, many free anti-virus product available that will do the job just fine. Please remember to keep your Anti-Virus policies up to date. At a minimum, you should check for updates every week.

Windows - Not Free

www.kaspersky.com

www.symantec-norton.com/australia

www.mcafee.com

Windows - Free

www.free.avg.com

www.free-av.com

www.avast.com

Mac OSX – Free

www.clamav.com

Linux/Unix – Free

www.clamav.com

Again, for assistance with Anti Virus product, contact the IT Department. As with Firewalls, support is provided on a best effort basis.

Operating Systems

ICMS recommends that you keep your operating system up to date with the latest software updates and patches. Failure to do so puts your PC at risk from malicious users. These users could gain control of your PC and access to your sensitive information such as banking. Please make sure to update your PC.

Internet Browsers

ICMS also recommended that you use certain internet browsers. Older versions of Internet Explorer have numerous vulnerabilities that will put your PC at risk. Also, older versions of Firefox and Safari have similar vulnerabilities. Please upgrade to the following versions:

Internet Explorer version 7

(This is a minimum. Version 8 is preferred)

Firefox version 3

Web and Email Monitoring

To the extent permitted by law, ICMS monitors internet access and employs technical measures to enforce restrictions to the access of inappropriate content. To ensure system reliability and adequate capacity, we routinely monitor the number of e-mails individuals send and receive both internally and externally.

Additionally, where permitted by law, we reserve the right to access, review, copy and delete any messages for any purpose and to disclose them to any person (internally or externally) as we see fit. We do not make a practice of this, however we can, and will in circumstances where we think it is either necessary or appropriate.

If there is a question regarding the appropriateness of your use of the college's Internet access, we will be able to identify the exact dates, times and web locations that you have accessed. Excessive use and/or violation of any standards or policies may be deemed abuse, and could result in suspension of Internet access and/or other disciplinary actions up to and including termination of employment or Suspension from College.

Acceptable Use

The International College of Management Sydney's Internet access and e-mail systems are intended as tools to be used for business and study purposes and should not generally be used for personal, non-business or study related activities. ICMS management allows staff and student's to use e-mail and browse the World-wide Web on a personal basis to an extent similar to use of other communications facilities such as the telephone, provided that all requirements of the college's information security standards and policies are complied with, and such use does not interfere with the performance of normal college activities. This access, where permitted, is a privilege, not a right of enrolment or employment. It should never be used for activities that would be considered inappropriate within our college climate.

You must not use the e-mail or Internet access to deliberately store, display, generate and/or pass on to others material whether in text, pictures or any other form which may be regarded as offensive on race, sex, gender, sexual orientation, national origin, religious or political beliefs, disability grounds, copyright circumvention and distribution.

Software Copyright

“The owner of the copyright has the exclusive right to copy the work” (Section 16 The Copyright, Designs and Patents Acts 1988).

This act and similar laws throughout the world, protect the rights of authors of all kinds of creative work, including computer software. That means it is illegal to copy software without the copyright owner’s permission.

Breaking the law could have serious consequences for you and the company threatening both yours and our reputation and future prosperity.

These tips will help ensure you are not violating copyright laws:

1. Don’t share software with students or colleagues to make copies.
2. Don’t make additional non-licensed copies if you are using a network.
3. Don’t make unauthorized copies of college’s-installed software to take home.
4. Don’t accept “free” software from colleagues or friends.
5. Open source software does not cost anything. This is a type of free software that is acceptable.