



ICMS Internet, Email and Information Security Policy

The Internet: Web Browsing and Email

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.

Various add-ins (e.g. Java applets, Active-X controls, Plug-ins etc...) are sometimes required in order to properly experience a particular web site. The first time you encounter any given add-in, you may be prompted with a 'certificate' that identifies the maker of the add-in. Unless the product is from Microsoft you must contact IT before attempting to install any such components on ICMS Computers.

You must not use the e-mail system 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.

Subject to local law, all electronic messages composed, sent and received via the ICMS' Internet access are and remain at all time the property of the ICMS.

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.

Storing Information on Shared Drives

All work and study related information should be saved to the appropriate shared drive. When using a portable computer, local files should be synchronized with a network location regularly – ideally each time you return to the college. Clear benefits of this are:

- information held on shared drives is backed up routinely
- if you are away from the college for any reason, data held on the shared drives is easily accessible by other team members if required

Software Purchases

The Company has volume licensing agreements in place for the purchase of many applications. Prior to purchasing any software, please consult the current list of agreements with the IT department to see if one may apply in your situation. IT must be involved in all software purchases and evaluations.

Unauthorized Software

Except as noted previously in the Internet policy under "Various add-ins..." no software may be loaded onto the college's PC's without prior approval from IT Support. Under no circumstances can anyone agree to terms and conditions online for software downloads that have not been pre-approved prior.

Without such approval, you may not install any software not provided by the ICMS including (but not limited to):

- programs given to you by colleagues or friends outside of the college
- discs or CD received through the post or with a magazine
- demonstration software
- any disc produced from your home or college computer
- any computer file transferred electronically from an outside source

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:

- Don't share software with colleagues to make copies.
- Don't make additional non-licensed copies if you are using a network.
- Don't make unauthorized copies of college's-installed software to take home.
- Don't accept "free" software from colleagues or friends.
- Do formally request software through approved purchase processes.
- Do request approval from the IT department before attempting to install any software.

Intellectual Property

All ICMS policies remain in force when using the Internet, including any confidentiality and non-disclosure agreements. All data produced and stored by the college is the property of ICMS and/or our clients.

Please consult our official local policy documents for full details, and such exceptions as may be applicable to your domain.

Password Security

Do not give your username and password to anyone, including IT staff. Do not write passwords down and leave in a place easily accessible by other people. Use a secure password and not one containing easily guessed information such as name, city, country, date of birth or phone number.

Anti-Virus Software

All computers provided by the college are configured with anti-virus software, which is managed and updated centrally by the IT department. You may not bypass or disable this software for any reason.

If you suspect that a virus or other malicious software has been introduced you must contact IT Support immediately. Speed is essential in order to restrict the spread of the virus.

On no account should you attempt to remove any infected files yourself.

