CONDITIONS FOR USE OF SILICA CLUSTER (11 Jun 2008)

Overview

Silica is a shared facility that is intended to operate with maximum utilisation and minimal management overhead. The Management Committee will have oversight of the general resource allocation and will liaise with Departmental representatives regarding resource utilisation. Each Department is expected to manage their own users as needed and in accordance with guidelines provided by the Management Committee.

The Management Committee is comprised of one representative from each of
• School of Chemistry
• School of Physics
• School of Chemical and Biomolecular Engineering (representing users from that School and the Faculty of Engineering & IT)
• School of Mathematics

Obligations of Supervisors with regards use of the Silica Cluster

In order to effectively manage the widely distributed users of the Silica Cluster, we require that each user be associated with a member of staff who will agree to serve as the Supervisor for that user. A staff member who is eligible to be a supervisor may, of course, act as their own supervisor, i.e. take on the responsibilities of a supervisor as well as a user.

1. In the context of Silica Cluster usage, a supervisor is an academic member of staff of a participating School or Department. It is expected that a student and postdoctoral user will use their actual supervisors in this context, a visitor user would still require a supervisor even though they may not actually be under any formal supervision.

2. Requests to the supervisor from the Cluster Management Committee, either directly or via their Departmental representative, for action or information concerning issues relating to use of Silica by themselves or users for whom they have agreed to act as supervisor will be acted upon promptly.

3. Issues that a supervisor wishes to raise concerning the use of Silica will be put to their Departmental representative of the Cluster Management Committee as the person best placed to assess the nature of the issue raised. Should it be a matter that the representative feels should be addressed by the Management Committee then the representative will be responsible for bringing it to the committee’s attention.

4. The Cluster Management Committee will levee funds from participating departments to cover incidental costs. This will be in the form of an annual fee per user and is indicated on the user application form. The supervisor will provide the annual fees for users that fall under their supervision as defined above to be collected by the departmental representative unless some alternative funding arrangement is agreed upon within the department.

Obligations of Users

What follows is Code of Conduct from the ICT website
Use of the University’s ICT Resources is restricted to legitimate University purposes only. For students this generally means academic coursework and research as approved by a supervisor. Staff usage will depend on the nature of their work. The use of University ICT Resources through non-University (including personally owned) equipment is also subject to this policy.

To assist Users to understand the implications of the above condition the following examples of prohibited and permitted use are provided. These examples are indicative only.

a) The University will not tolerate its ICT Resources being used in a manner that is harassing, discriminatory, abusive, rude, insulting, threatening, obscene or otherwise inappropriate.

It is illegal to use any ICT Resource to harass, menace, defame, libel, vilify, or discriminate against any other person within or beyond the University. It is important to understand that in matters of discrimination and harassment it is the reasonable perception of the recipient and not the intention of the sender that is significant.

Users may be individually liable if they aid and abet others who discriminate against, harass or vilify colleagues or any member of the public. Users who adversely affect the reputation of another person may be sued for defamation by that aggrieved person.

b) Users must not use the University’s ICT Resources to collect, use or disclose personal information in ways that breach the University’s Privacy Policy.

c) Users must respect and protect the privacy of others.

d) Users are forbidden to use ICT Resources to access, store or transmit pornographic material of any sort other than with specific written approval from an authorised University Officer for research related purposes.

e) The use of ICT Resources for gambling purposes is forbidden.

f) The University forbids the use of its ICT resources in a manner that constitutes an infringement of copyright. The law permits copying and/or printing only with the permission of the copyright owner, with a few very limited exceptions such as fair use for study or research purposes (this exception itself is subject to numerous provisos and conditions in the Copyright Act).

Accordingly Users must not download and/or store copyright material, post copyright material to University websites, transfer copyright material to others or burn copyright material to CD ROMs or other storage devices using ICT Resources, unless the copyright material is appropriately licensed. Copyright material includes software, files containing picture images, artistic works, live pictures or graphics, computer games, films and music (including MP3s) and video files.

g) ICT Resources must not be used to cause embarrassment or loss of reputation to the University.

h) The University does not permit the use of its ICT Resources for unauthorised profit making or commercial activities. Academic staffs are referred to the
University’s Outside Earnings Policy with regard to the use of University Resources for private professional practice. General staff are referred to the University's Code of Conduct.

i) All internet content made available on the University’s ICT Resources must comply with the University’s policy on Internet Content.

j) Users must not use ICT Resources in inappropriate ways, which are likely to corrupt, damage or destroy data, software or hardware, either belonging to the University or to anyone else, whether inside or outside the network. They may only delete and alter data as required by their authorised University activities.

Note: This does not apply to specially authorised University computing staff who may be required to secure, remove or delete data and software, and dispose of obsolete or redundant ICT Resources as part of their ICT Resource management duties.

k) Users must not attempt to repair or interfere with, or add any devices (whether hardware or components) to, any ICT Resource, unless they are authorised and competent to do so. All faults or suspected faults must be reported to either the relevant departmental computer services officer or IT Services Helpdesk.

l) ICT Resources must not be used to distribute unsolicited advertising material from organisations having no connection with the University or involvement in its activities.

m) Users of University issued accounts must identify themselves and not use a false identity.

n) University email lists generated for formal University communications must not be used for other than University business.

o) Unless via a personally paid account, files may only be accessed or downloaded if they are work or study related. In any case, files may only be downloaded if it is legal to do so and steps have been taken to ensure that the files are free from viruses and other destructive codes.

p) Files may only be attached to email messages if the sender believes they are free from viruses and has taken steps to ensure that they do not contain viruses or other destructive code.

q) Users must not attempt to gain unauthorised access to any computer service. The use of another person's login, password or any other security device (e.g. SecurID, digital signature or biometric identification) is not permitted. Nor must Users exploit any vulnerability in systems or (except authorised staff when checking security of systems as part of their duties) use any technology designed to locate such vulnerabilities or circumvent security systems. Such behaviour is likely to be a breach of Part 6 of the NSW Crimes Act 1900 and if proven would potentially be considered serious misconduct and accordingly may be dealt with under relevant disciplinary provisions. The matter may also be referred to the police and/or the Independent Commission Against Corruption.

r) Users must not use ICT Resources for the purposes of subscribing to and accessing fee based services that are for personal use only, unless the
subscription or access is from a personally paid account and the Users personally pay the fees for the services and the services are legal.

s) Users must not facilitate or permit the use of the University’s ICT Resources by persons not authorised by the University e.g. Users must not set up a wireless relay base station from their University accounts.

t) Local members of associations (including authorised delegates of unions which are parties to the University’s Enterprise Agreements) may make reasonable use of the University’s ICT Resources for communicating with the University and for internal union(s) communications relating to enterprise bargaining, other related local negotiations or for matters affecting an individual staff member.

u) Limited minor and incidental personal use may be allowed, but it is a privilege and must not interfere with the operation of ICT resources, burden the University with incremental costs, interfere with the User’s employment or other obligations to the University and is subject to compliance with University policies. Users should be aware that personal use of the University’s ICT Resources may result in the University holding personal information about the User and/or others which may then be accessed and used by the University to ensure compliance with this, and other policies.

Monitoring

a) Use of ICT Resources is not considered private. Users of ICT Resources should be aware that they do not have the same rights as they would using personally owned equipment through commercial service providers.

b) The University's electronic communication systems generate detailed logs of all transactions and use. All users should be aware that the University has the ability to access these records and any backups. In addition, system administrators have the ability to access the content of electronic communications and files sent and stored using the University's equipment.

c) The University charges telephone calls and Internet charges back to schools/departments. This means that managers are regularly advised of postal expenditure, the costs of all telephone calls from each extension and Internet traffic costs associated with each network connection/computer. Users should be aware that details of telephone numbers called are recorded and can be accessed.

d) The University reserves the right to audit regularly and monitor the use of its ICT Resources to ensure compliance with this policy.

e) The University also reserves the right to look at and copy any information, data or files (including non-University material) created, sent or received by Users using, or while connected to, the University’s ICT Resources in the event of a suspected breach of this or other policies.

Response to Breaches

a) The University reserves the right to withdraw, restrict or limit any User’s access to its ICT Resources if a breach of these conditions is suspected. Any such suspected breach may also be investigated under other University
processes, and may result in disciplinary action being taken against the offender in accordance with those processes. This may include a request to reimburse costs (e.g. for unreasonable personal use), disciplinary action (including termination of employment/suspension of candidature) and/or criminal prosecution.

b) Further the University reserves the right to remove or restrict access to any material within the University domain. Such decisions will be communicated to the appropriate supervisor and account holder.

Security, Confidentiality and Privacy

a) Matters of a confidential nature should only be conveyed or stored in an electronic format when adequate security measures have been taken.

b) While the University communications systems are electronically safeguarded and maintained in accordance with current best practice, no guarantee can be given regarding the protection confidentiality, privacy or security of any information.

c) Email and other records stored in ICT Resources may be the subject of a subpoena, search warrant, discovery order or application under the NSW Freedom of Information Act 1989. Disclosure outside the University of any personal information, irrespective of its format, will be in accordance with the NSW Privacy and Personal Information Protection Act 1998, the Health Records and Information Protection Act 2002, the University's Privacy Policy and its Privacy Management Plan.

d) While the NSW Privacy and Personal Information Protection Act, and the NSW Health Records and Information Protection Act 2002 and the expression of these in the University Privacy Policy, regulate the collection, management, use, security and disclosure of personal information, the Act and the Policy do not confer an automatic right of privacy for Users accessing ICT Resources. The University may collect and receive personal information of Users and others in the course of managing the operation and use of its ICT Resources and that information can be used in connection with efforts to ensure that Users comply with all relevant laws and University policies.

e) Communications on University business in any format or media are official records, subject to statutory record keeping requirements and the University Recordkeeping Policy. This includes email sent and received by staff members on any University related matter. Staff need to be conscious of the need to preserve official communications in accordance with the relevant University guidelines on the management of electronic records. Care should be taken before deleting any electronic communication that it is not required to be kept as evidence of a decision, authorisation or action.

f) Sending an email on an official University matter is similar to sending a letter on University letterhead. Such email transactions should be handled with the normal courtesy, discretion and formality of all other University communications. Users should not write anything in an email that they would not sign off in a memorandum.