UNIVERSITY OF CANBERRA

UNIVERSITY FACILITIES (INFORMATION AND COMMUNICATION TECHNOLOGY NETWORK) RULES 2006

PART 1 – PRELIMINARY

Citation

1. These Rules are the University Facilities (Information and Communication Technology Network) Rules 2006.

Commencement

2. These Rules commence on the commencement of the University of Canberra (University Facilities) Amendment Statute 2006.

Revocation and determinations

3. (1) The Computer Services Centre Rules 1993 are revoked.

(2) Determinations made under the *Computer Services Centre Rules 1993* are deemed to have been made under these Rules and continue in force until those determinations or these Rules are revoked.

Interpretation

4. (1) In these Rules, unless the contrary intention appears:

"account" means a computer account assigned to a user under rule 5;

"child" means a person under the age of 18 years;

"Dean of Students" means the member of staff appointed as Dean of Students;

"Director" means the Director of an administrative service or commercial unit of the University, not including a Division;

"Division" means a Division of the University headed by an Executive Director or Pro Vice-Chancellor;

"general access laboratory" means a room designated as such under rule 15;

"hardware" means the computer and communications equipment, components, parts of components and operating manuals of the University including network access ports, whether wired or wireless, remote and portable computer and communications equipment such as mobile telephones, laptop computers, personal digital assistants and the like owned or provided by the University and any private equipment connected to the University's ICT network;

"information" means data held electronically on any part of the ICT network;

"identity card" means an identity card issued by the University to a member of staff or a student of the University;

"ICT network" means the University information and communication technology network, including hardware, software and information as defined in these Rules, and all cabling linking the hardware. It includes wired, wireless, microwave and similar technologies used to link and access the hardware and software;

"limited personal use" means use of the ICT network in accordance with the policy and guidelines on limited personal use;

"member of staff" means a member of the academic staff or the general staff of the University;

"prohibited room" means a room designated as such under subrule 14(1);

"**Rights Holder**" means an owner or exclusive licensee of a relevant copyright under the *Copyright Act 1968 (Cth)*;

"Senior Manager" means an Executive Director, Pro Vice-Chancellor or Director;

"software" means licensed software products and computer programs and includes any updates and new releases of products;

"supervisor" means a member of staff for the time being in charge of any area of the University described in these Rules as part of the ICT network of the University;

"URL" means the Uniform Resource Locator of a website;

"user" means a person who accesses the ICT network whether that access is from within the University or from outside the University;

(2) A reference in these Rules to a decision includes a reference to:

(a) granting, refusing to grant, suspending or revoking a permission, or imposing terms or conditions, under rule 14, 16 or 17; and

(b) giving a direction under rule 14, 16 or 17; and

(c) waiving or refusing to waive the whole or a part of a penalty under rule 20 or 21; and

(d) affirming, varying, setting aside or making a decision under rule 22.

PART 2 – ACCESS TO AND USE OF THE INFORMATION AND COMMUNICATION TECHNOLOGY NETWORK

Authorised Access and Use

5. (1) A person must not use the ICT network unless he or she is authorised to do so by a Senior Manager.

(2) It is a condition of the authorisation referred to in subrule (1) that the user must comply with the conditions, and have regard to the policy and guidelines, on the use of and access to the University's ICT network issued by the Vice-Chancellor or a Senior Manager from time to time.

(3) A person commits an offence if the person:

(a) uses the ICT network, or any part of the ICT network, without being authorised to do so; or

(b) obtains access to information without being authorised to do so; or

(c) uses another user's account except where the usage forms part of a maintenance or support job authorised by a Senior Manager; or

(d) uses, for purposes other than those identified in subrule (4), facilities which he or she is authorised to use; or

(e) uses or accesses the ICT network contrary to the conditions, policy and guidelines identified in subrule (2).

(4) Except for limited personal use, a person must use the ICT network only in relation to the educational, research and administrative business of the University.

(5) A person who contravenes subrule (4) commits an offence.

(6) Notwithstanding rules 16 and 17, the University may establish conditions for access and use of the ICT network, including the imposition of charges or quotas.

(7) A user who exceeds a quota imposed by conditions established under subrule (6) must pay to the University a charge and, in relation to the amount to be recovered, rules 20, 21 and 24 shall apply as if the amount of the charge were a monetary penalty imposed under rule 20.

(8) An officer nominated by a Senior Manager may assign an account to a user to enable the user to access that part of the ICT network for which the account is required.

Passwords

6. A person commits an offence if he or she is in possession of a username and password that in combination give access to any part of the ICT network and:

- (a) uses them to obtain access without authorisation; or
- (b) discloses them to another person.

Use for Gain

7. A person who knowingly or recklessly uses any part of the ICT network for private gain, or for a financial gain to a third party, commits an offence unless authorised under the conditions, policy and guidelines issued under subrule 5(2).

Copying and Copyright

8. (1) A user of the ICT network commits an offence if he or she copies:

- (a) the information of another user contained on the ICT network (without the consent of the other user); or
- (b) any software contained on the ICT network (without the consent of the licensor of the software); or

(c) information belonging to the University which the user is not authorised to access; or

(d) information and thereby infringes or facilitates the infringement of copyright material in breach of the *Copyright Act 1968 (Cth)*; or

(e) information external to the University in breach of any licences held by the University providing for online access to that information by authorised users.

(2) If, in the course of any systems management monitoring of network traffic, filtering that traffic, using file detection technologies or exercising any other network or systems management capability, an authorised officer of the University detects files which include or may include infringing material under subrule (1)(d), a Senior Manager may authorise the quarantining or removal of such material from the ICT network.

(3) If a Rights Holder or authorised representative of a Rights Holder informs an appropriate authorised officer of the University that a file in the ICT network contains a reproduction or communication of allegedly infringing material under subrule (1)(d), a Senior Manager may authorise the quarantining or removal of such material from the ICT network.

(4) If a Senior Manager acts under subrules (2) or (3) in good faith on a belief held on reasonable grounds, such officer of the University and the University shall not be liable for any damage resulting from the quarantining or removal of materials under subrules (2) or (3).

Interfering or Subverting

9. (1) A user must not interfere with the operation of the ICT network or any part of the ICT network.

(2) If a user wilfully causes interference with the operation of all or part of the ICT network, he or she commits an offence.

(3) If a person attempts to subvert the security of any part of the ICT network, he or she commits an offence.

(4) Any person who without authority or excuse:

(a) destroys, erases or alters information stored in, or inserts information into, the ICT network or any part of the ICT network; or

(b) interferes with, or interrupts or obstructs the lawful use of, a part of the ICT network; or

(c) destroys, erases, alters or adds information stored on behalf of the University in a computer that is not a University computer; or

(d) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in the ICT network or information stored on behalf of the University in a computer that is not a University computer;

commits an offence.

(5) A user who, in particular circumstances, commits an offence to which subrules (2) and (4) would, but for this subrule, both apply, is only to be regarded as committing an offence under one of those subrules in respect of those particular circumstances.

(6) A person authorised by a Senior Manager may take action to stop any equipment in the University found to be interfering with the operation, or subverting the security, of any part of the ICT network from continuing to do so. Such action may include switching off, disconnecting and removing the equipment.

Obscene, Offensive, etc. Messages or Material

10. (1) The ICT network must not be used:

- (a) in a manner that brings the University into disrepute; or
- (b) to send or communicate obscene, offensive, harassing or defamatory messages or material to another person whether at the University or at another place.

(2) If a user sends or communicates a message or material referred to in subrule (1), whether within the University or to a person outside the University, on a network connected to the ICT network, whether it identifies the user as affiliated with the University or not, the user commits an offence.

(3) If a user sends, through equipment which is not a University computer or facility, a message or material to which subrule (1) applies and which associates the name of the University with the message or material, the user commits an offence.

Misrepresentation

11. A person who represents himself or herself as another person, whether fictional or not:

- (a) to obtain access to the ICT network or any part of it; or
- (b) to purport to be the author of any work or information on the ICT network, or
- (c) to send any message or information on the ICT network;

commits an offence.

Damage to Items

12. A person who wilfully or recklessly:

(a) damages any item, article or part of any ICT network; or

(b) erases, deletes or damages any information on the ICT network, other than information in their own account;

commits an offence.

Power to Remove Material

13. (1) If in the course of any systems management monitoring of network traffic, filtering that traffic, using file detection technologies or exercising any other network or systems management capability, an authorised officer of the University detects files which include or may include material which contravenes these Rules or any law or the policies or guidelines of the University, a Senior Manager may authorise the quarantining or removal of such material from the ICT network.

(2) If a person informs an appropriate authorised officer of the University that a file in the ICT network includes or may include material which contravenes these Rules or any legislation or the policies or guidelines of the University, a Senior Manager may authorise the quarantining or removal of such material from the ICT network.

(3) If a Senior Manager acts under subrules (1) or (2) in good faith on a belief held on reasonable grounds such officer of the University and the University shall not be liable for any damage resulting from the quarantining or removal of materials under subrules (1) or (2).

PART 3 - ROOMS AND LABORATORIES

Prohibited Rooms

14. (1) For the purposes of these rules, a Senior Manager may, by writing signed by the Senior Manager, designate a room to be a prohibited room. Such a room may include adjacent space, such as corridors, toilets, store rooms, tea rooms and foyers used primarily to support or facilitate the ICT network in the University.

(2) Subject to subrule (3), no person is permitted to enter a prohibited room, other than a member of staff authorised by the Senior Manager or a person who is invited to enter such a room by such a member of staff.

(3) The Senior Manager may grant permission to a person to enter a prohibited room and may, at any time, suspend or revoke the permission.

(4) The grant of permission under subrule (3) may be subject to such terms and conditions, if any, as the Senior Manager considers appropriate.

(5) A supervisor may direct any person, other than a member of staff or a person to whom permission has been granted under subrule (3), to leave a prohibited room and may take such action as is reasonably necessary in all the circumstances to ensure

compliance with any such direction.

(6) It is an offence under these Rules for a person to fail to comply with a direction given under subrule (5).

General Access Laboratories

15. For the purposes of these rules, a Senior Manager may, by writing signed by the Senior Manager, designate a room to be a general access laboratory. Such a room may include adjacent space, such as corridors, toilets, store rooms, tea rooms and foyers used primarily to support or facilitate the ICT network in the University.

Powers of a Senior Manager

16. (1) For the purposes of these Rules, a Senior Manager may, by writing signed by the Senior Manager:

(a) determine the general terms and conditions under which, and the procedures by which, users may:

(i) operate or use any equipment in, or any services of, prohibited rooms and general access laboratories; or

(ii) borrow any equipment or other item from the prohibited rooms and general access laboratories; or

(iii) have access to a prohibited room or general access laboratory; and

(b) vary any terms, conditions or procedures determined under paragraph (a); and

(c) determine, from time to time, the days on which, and the hours during which, the prohibited rooms and general access laboratories, are to remain open or be closed; and

(d) determine, from time to time, the days on which, and the hours during which, any specified equipment in, or services of, the prohibited rooms and general access laboratories are to be available for operation or use; and

(e) determine, from time to time, charges applying for access to prohibited rooms and general access laboratories.

(2) The Senior Manager may take such action as is reasonably necessary in all the circumstances for the purpose of carrying out a decision made by him or her under these Rules.

(3) It is an offence under these Rules for a person to fail to comply with a term or condition as determined or varied under subrule (1).

Powers of the Supervisor

17. (1) The supervisor may require any person in a prohibited room or general access laboratory to produce evidence of his or her entitlement:

(a) to operate or use any equipment in, or any services of, prohibited rooms and

general access laboratories; or

(b) to borrow equipment or other items from prohibited rooms and general access laboratories; or

(c) to have access to prohibited rooms and general access laboratories.

(2) If a person fails to comply with a requirement under subrule (1), the supervisor may direct that person to leave the prohibited rooms and general access laboratories and that person must not, subject to subrule (3), re-enter the prohibited rooms and general access laboratories until he or she has produced evidence of such entitlement.

(3) A person to whom a direction has been given under subrule (2) may re-enter the prohibited rooms and general access laboratories for the purpose of producing such evidence.

(4) Where the supervisor is satisfied that a person has committed a breach of a provision of rule 18, the supervisor may recommend that a Senior Manager direct that person to leave the prohibited rooms and general access laboratories for such period, not exceeding 24 hours, as the Senior Manager determines.

(5) A person directed to leave the prohibited rooms and general access laboratories under subrule (4) must not re-enter the prohibited rooms and general access laboratories until the expiration of the period determined under that subrule.

(6) The supervisor may, if the supervisor considers it appropriate to do so, on such terms and conditions as are, from time to time, determined by a Senior Manager, grant permission to any person to:

(a) display or distribute in the prohibited rooms and general access laboratories any notice or pamphlet; or

(b) organise or take part in a gathering in the prohibited rooms and general access laboratories; or

(c) organise, mount or attend an exhibition in the prohibited rooms and general access laboratories; or

(d) remove from the prohibited rooms and general access laboratories any equipment or other item held in the prohibited rooms and general access laboratories that is not available for borrowing by that person; or

(e) operate or use any equipment in, or services of, the prohibited rooms and general access laboratories otherwise than in accordance with normal operating or using procedures of the prohibited rooms and general access laboratories as determined under rule 16; or

(f) remove any equipment or other item from the prohibited rooms and general access laboratories otherwise than in accordance with the normal borrowing procedures of the prohibited rooms and general access laboratories as determined under rule 16; or

(g) have access to prohibited rooms and general access laboratories otherwise than in accordance with the access terms, conditions and procedures as determined under rule 16; and may, in like manner, suspend or revoke a permission so granted.

(7) The supervisor may take such action as is reasonably necessary in all the circumstances for the purpose of carrying out a decision made by the supervisor.

(8) It is an offence under these Rules for a person to fail to comply with a direction given under this rule.

Prohibited Conduct

18. (1) A person must not, without the permission of a supervisor, act in contravention of any terms, conditions or procedures determined by a Senior Manager under rule 16.

(2) A child, other than a child who is a student of the University or a member of staff, must not enter or remain in any room or other area covered by a determination made under these Rules except:

- (a) with the permission of a supervisor, and
- (b) under the control of an adult at all times.

(3) It is an offence for a person to breach subrule (1) or allow a breach of subrule (2).

PART 4 – PENALTIES

Offences

19. A person who:

- (a) commits an offence; or
- (b) repeats an offence; or
- (c) otherwise contravenes a provision of these Rules;

is liable to a penalty set out in rule 20.

Penalties

20. (1) Subject to rule 21, if a Senior Manager finds that a person has committed an offence, the Senior Manager may, in relation to the offence:

- (a) decide to take no action;
- (b) reprimand the person committing the offence;

(c) with the consent of the Vice-Chancellor, suspend the person from the use of all or part of the ICT network under their management;

- (d) with the consent of the Vice-Chancellor, close the relevant account;
- (e) recommend to the Vice-Chancellor (or the delegate of the Vice-Chancellor)

that the person be dealt with for misconduct:

(i) if the person is a student of the University – under the *Regulation of Student Conduct Rules 1992*; or

(ii) if the person is a member of staff – under the relevant industrial award or Australian Workplace Agreement;

(f) determine the conditions under which the person may have access to the ICT network;

(g) determine compensation payable by the person to the University for damage to the ICT network; or

(h) determine compensation payable by the person to the University for the failure to return hardware or software by the date determined under rule 16(1); or

(i) take any action, being a combination of the actions specified in paragraphs (b) to (h) (inclusive).

(2) If the Senior Manager determines under paragraph (1)(g), (h) or (i) that compensation is payable by a person, the person must pay to the University such amount as the Vice-Chancellor determines not exceeding:

(a) the lesser of:

(i) an amount equivalent to the cost of the repair of the damage; and

(ii) \$5,000; or

(b) if the damage is irreparable or an item borrowed under the conditions determined under rule 16(1) is not returned by the specified date – the lesser of:

(i) an amount equivalent to the cost (including any reasonable administrative cost) of replacing the item or article or part of the ICT network, as the case may be; and

(ii) \$5,000

(3) Nothing in subrule (2) prevents the University from recovering, in a court of competent jurisdiction, that part of:

(a) the amount of the cost of the repair of the damage caused by a person; or

(b) the amount equivalent to the cost (including any reasonable administrative cost) of replacing the item or article or part of the ICT network damaged by the person (as the case requires) that exceeds \$5,000.

(4) The Vice-Chancellor may, in relation to an offence for which the sole penalty is a monetary penalty:

(a) waive or reduce the monetary penalty payable for the offence; or

(b) extend the time for the payment of the monetary penalty.

(5) If a person becomes liable to pay to the University a monetary penalty or other

amount under this rule, the person must pay to the University the amount specified in the notice given under subrule 21(3) in relation to the matter not later than 1 month after:

(a) if an appeal is not lodged under rule 24 in relation to the finding giving rise to the liability – the date of the notice; or

(b) if an appeal is lodged under rule 24 in relation to the finding giving rise to the liability – the day on which the decision is given in respect of the appeal.

(6) A person who is liable to pay to the University a monetary penalty or other amount under this rule, is not entitled to use the ICT network, unless otherwise authorised in writing by the Senior Manager, if the amount remains unpaid after the time referred to in subrule (5) has expired.

(7) A determination made for the purposes of this rule must be in writing and must be given to the person in relation to whom it is made.

Imposition of Penalties

21. (1) If it appears to a Senior Manager that a person is in breach of these Rules, the Senior Manager, acting with the agreement of the Vice-Chancellor (or the delegate of the Vice-Chancellor), may immediately suspend the person from use of the ICT network for an initial period not exceeding 28 days.

(2) A suspension under subrule (1) takes effect as soon as written notice of it is given or delivered to the person suspended.

(3) A penalty (other than a suspension referred to in subrule (1)) must not be imposed on a person unless:

(a) the person is given written notice of:

(i) the breach that is alleged to have been committed by the person; and

(ii) the penalty that is proposed to be imposed for the alleged breach in addition to any suspension under subrule (1); and

(b) the notice is accompanied by a copy of this rule and of rule 24; and

(c) a period of not less than 7 days, or any shorter period that is agreed to by the person, has elapsed since the giving of the notice; and

(d) any written representations made, during the period referred to in paragraph (c), by the person to the Senior Manager about the alleged offence or the proposed penalty, or both of them, have been taken into account; and

(e) in the case of a person who appeals against a finding or penalty under rule 24 -the decision of the Appeals Committee is given to the appellant and the Senior Manager under subrule 24(10).

PART 5 – APPEALS AND REVIEWS

Review of Decisions of Supervisor

22. (1) Where a person is dissatisfied with a decision of a supervisor made in the exercise of a power conferred by rule 16 or 17 or subrule 14(5), the person may apply in writing to the Senior Manager for review of the decision;

(2) The Senior Manager must, as soon as practicable after receiving an application under subrule (1), review the decision in such manner as the Senior Manager considers appropriate and may:

(a) affirm, vary or set aside the decision under review; or

(b) set aside the decision under review and make a decision in substitution for that decision;

as the justice and the merits of the case require.

ICT Network Appeals Committee

23. (1) There is to be an Information and Communication Technology Network Appeals Committee.

(2) Subject to subrule (3), the Committee consists of the Chair and 3 persons selected by the Vice-Chancellor, for the purposes of an appeal, from the following persons:

- (a) the Dean of Students;
- (b) a nominee of the Vice-Chancellor;

(c) a person appointed after consultation with the University of Canberra Students' Association or its successor;

- (d) the members of the Council;
- (e) members of the general staff of the University.

(3) A person is not eligible to be selected as a member of the Committee, for the purposes of an appeal, if that person is a member of staff (including the part-time and casual staff) of the same Division as the appellant.

(4) The Chair of the Committee is appointed by the Vice-Chancellor.

(5) An appointment of the kind referred to in paragraphs (2)(b), (c), (d) and (e) must be in writing signed by the person making the appointment and delivered to the Chair of the Committee.

(6) A quorum at a meeting of the Committee is the Chair and 2 other members.

Appeals to Appeals Committee

24. (1) If the Senior Manager finds that a person has committed an offence against these Rules, the person may appeal to the Committee against the finding and, if a penalty was imposed in respect of that breach, against the penalty.

(2) An appeal must be lodged within 14 days of the date of the finding by delivering a notice of appeal to the Vice-Chancellor who must forward the notice to the Chair of the Appeals Committee.

(3) The procedure at a hearing by the Committee may be determined by the members of the Committee present at the hearing.

(4) The Committee is not bound to act in a formal manner but, subject to this rule, may inform itself on any matter in any manner as it thinks just.

(5) The Committee must disregard any statement that appears to it to have been obtained unfairly or to which, in the opinion of the Committee, it would be unjust to have regard.

(6) At a hearing by the Committee, the appellant is entitled to be accompanied by a person nominated by the appellant, being:

- (a) a student; or
- (b) a member of staff; or
- (c) a member of a registered trade union

except a person who is a qualified lawyer.

(7) A person referred to in subrule (6) may:

(a) advise the appellant in relation to the appeal; and

(b) address the Committee and examine and cross-examine witnesses on behalf of the appellant.

(8) After receiving the evidence and representations advanced by the appellant and any other evidence, about either or both of:

(a) the finding of the Senior Manager; and

(b) the penalty (if any) imposed by the Senior Manager;

the Committee may:

- (c) confirm the decision; or
- (d) vary the decision; or

(e) set aside the decision and make a decision in substitution for the decision set aside; or

(f) set aside the decision.

(9) If the Committee is divided in opinion as to the decision to be made on any question, the question must be decided:

(a) if the members of the Committee present and participating in the making of the decision are not equally divided in opinion – according to the opinion of the majority; and

(b) if those members are equally divided in opinion – in favour of the appellant.

(10) The decision of the Committee and the reasons for the decision must be given in writing to the appellant and the Senior Manager within 7 days of the making of the decision.

(11) An appeal hearing under these Rules is not ineffective by reason only of a formal defect or irregularity in the convening or conduct of the Committee.

(12) The decision of the Committee is final.

PART 6 – MISCELLANEOUS

Delegation by a Senior Manager

25. (1) A Senior Manager may, in writing, delegate to a supervisor all or any of his or her powers or functions under these Rules, other than his or her powers and functions under rules 22 and 25.

(2) A delegation under this rule is revocable in writing.

Personal Information

26. The University collects or receives personal information of users. In the course of managing the operation and use of the ICT network the University is authorised to use that information in connection with efforts to ensure that their use and that of other users complies with all relevant legislation and University policy and guidelines.

Monitoring and Recording Access and Use and Content

27. (1) The University is authorised to monitor and record all access to and contents of the ICT network and to retain such records. The University may use such records and information in accordance with the provisions of these Rules.

(2) The monitoring and recording includes but is not restricted to:

(a) URLs of sites visited, the date and time they are visited and the duration of site visits. Network addresses accessing URLs (including caches) and the URL address are recorded and may be correlated;

(b) e-mail messages, including the date and time the message was transmitted, received and opened and the e-mail address of the sender and recipients;

(c) use of the news server, both by access to newsgroups and by network address accessing the server and may correlate particular newsgroups to particular addresses;

(d) access to secured rooms and buildings by identity card, logins to servers and failure/security reports on all systems;

(e) telephone numbers and contact details of all calls made from University owned and provided telephones, including mobile telephones, and telephone numbers and contact details for all calls made to University owned and provided telephones, including mobile telephones;

(f) all financial accounts and invoices and vendor reports relating to the use of the ICT network;

(g) all network data including date, time, source, destination and content.

Reporting Breaches

28. (1) Persons are expected to report suspected breaches of Commonwealth or Australian Capital Territory laws and University legislation, policy and guidelines, and any unacceptable behaviour which occurs at the University or by a person acting in his or her capacity as a member of the University. Reports should be directed to an Executive Director or Pro Vice-Chancellor and are treated in a confidential and responsible manner. Reports are referred to the appropriate University authority for investigation or referred to the appropriate external agency.

(2) The University will protect the interests of any member of staff or student reporting a suspected breach in good faith and in a responsible way.

Publication of Rules etc.

29. The Pro Vice-Chancellor responsible for the ICT network must:

(a) cause copies of these Rules and of any conditions, policy and guidelines, as amended and in force for the time being, to be readily available in the University to users of the ICT network; and

(b) take all reasonable steps to ensure that the contents of the Rules and of any conditions, policy and guidelines are brought to the attention of all users of the ICT network.

Notices

30. For the purpose of these Rules, a notice or communication that is hand-delivered or sent by electronic or printed post to a person at a place shown in the records of the University as the person's:

- (a) semester address; or
- (b) work address; or
- (c) permanent home address; or
- (d) e-mail address

is regarded as having been given to the person on the date on which the notice was hand-delivered or, if it is sent by post, on the date on which it would, in the ordinary course of post, have been delivered to the person.

Application of Regulation of Student Conduct Rules 1992

31. Nothing in the Rules excludes the operation of the provisions of the *Regulation of*

Student Conduct Rules 1992 in relation to a breach of these Rules.

Notes

University Facilities (Information and Communication Technology Network) Rules 2006

Made by Council under section 4 of the *University Facilities Statute 1992* at meeting no. 107 on 2 August 2006.