

This speedsheet is to be used in conjunction with the Wireless Access Conference Delegate Information Sheet.

A copy of this information sheet can be accessed from the ITS website
<http://www.its.qut.edu.au/assist/conferences/guide>

Confernece Delegate account list

| ACCESS_NAME | PASSWORD | Delegate name |
|--------------------|-----------------|----------------------|
| qutcf001 | hello1207 | John Smith1 |
| qutcf002 | hello1208 | John Smith2 |
| qutcf003 | hello1209 | John Smith3 |
| qutcf004 | hello1210 | John Smith4 |
| qutcf005 | hello1211 | John Smith5 |
| qutcf006 | hello1212 | John Smith6 |
| qutcf007 | hello1213 | John Smith7 |
| qutcf008 | hello1214 | John Smith8 |
| qutcf009 | hello1215 | John Smith9 |
| qutcf010 | hello1216 | John Smith10 |

QUT Access Details

Below is the QUT Access username and temporary password that will allow you to access the Internet via QUT's wireless network for the duration of the conference.

Delegate Name: John Smith1

Username: qutcf001

Password: hello1207

By using this username and password you are agreeing to QUT's Information Facilities Rules. Acceptable use of information facilities is listed on the next page, and for the full version of the rules visit

<http://www.mopp.qut.edu.au/Appendix/append01cit.html>

Getting Connected

1. Use your computers wireless software to make a connection to "**QUT-Wireless**". Check your wireless network connection is enabled, and you are in an area that has wireless coverage.

2. Start a web browser (eg. Internet Explorer, Safari) and go to any external web page. You will then be redirected to this page: (Fig.1) You may wish to bookmark this page for later reference.



Fig. 1

3. Install the QUT SAS software by clicking on the appropriate link for your operating system under the heading **Software Downloads**, then click **Run**. You will only need to do this once. Once installed you need to reboot, then continue following these steps. Detailed instructions are available under the heading **User Guides**.
4. Check that your wireless connection to "**QUT-Wireless**" is re-established. Start the program **QUT Secure Access Service Client** (QUT SAS Client).
5. Select **On Campus Wireless** from the drop down menu on the left, and click **Connect**. (Fig. 2)

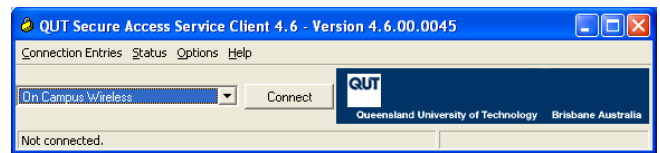


Fig. 2

6. Enter your QUT Access username and password, then click **OK**. Click **Continue** once you have read the banner. You are now connected to QUT's wireless network.
7. The QUT Access password given above must be changed before the account can be used. Go to www.qut.edu.au, and click **Computer accounts** from the "Quicklinks" menu. Log in with your QUT Access username and password. Ensure you have read the Information Facilities Rules, then tick the **I Accept** box and click **Submit**. Follow the prompts to change your password.

TIP! Always keep your password secure, do not write it down or give it to anyone. Visit <http://www.its.qut.edu.au/itsecurity/secure/passwords.jsp> for hints on picking a good password.

8. To access the Internet, start a web browser and go to a **non-QUT website**. Enter your QUT Access username and password at the Internet Access login, and click **Login**. Click **Activate** to connect to the Internet. A "Keep Alive" pop-up window will open behind your browser, and the website you wish to visit will be displayed. You must enable pop-ups from *.qut.edu.au to allow the "Keep Alive" window to open. Visit <http://www.its.qut.edu.au/assist/userguides/ias/ias.pdf> for information about accessing the Internet.

Please note that you will not be able to establish a VPN connection to any other organisation or corporate network while connected to Wireless at QUT.

Getting Help

If you require IT support please contact:

Name: IT Support Officer 1
Location: GP
Telephone: 3138 4000
Mobile: 123456789

Name: IT Support Officer 2
Location: GP
Telephone: 3138 4000
Mobile: 123456789

ACCEPTABLE USE OF INFORMATION FACILITIES

1. Purpose of this schedule

The object of this schedule is to promote ethical and responsible use of the university's information facilities.

2. Definition

In this schedule -

"QUT access account" means the account allocated by the university to a user to access information technology services and information.

3. Use of information facilities to comply with law

A user must use the university's information facilities in a manner which is consistent with the laws of the Commonwealth and the State of Queensland, including the following -

- (a) laws relating to copyright, intellectual property, and the ownership of data, information and software;
- (b) laws relating to harassment, discrimination, defamation, breach of confidence and the protection of personal privacy;
- (c) the criminal laws of the Commonwealth or the State of Queensland;
- (d) Schedule 1 (Part 3, section 12) of the [Queensland University of Technology Act 1998](#) .

4. Behaviour while using information facilities

(1) A user must not, while using the university's information facilities -

- (a) bring food into or eat, drink or smoke in a physical space comprising an information facility, unless the area is designated for those purposes; or
- (b) create a nuisance to other users by generating excessive noise in a physical space, whether from talking, music, electronic games or other activities; or
- (c) overload or monopolise information facilities, including equipment, space or services, in a manner which adversely affects other users; or
- (d) bring an animal (other than a guide dog) into a physical space comprising an information facility; or
- (e) physically interfere with or damage property or equipment of the university or other users whilst using an information facility.

(2) If requested by a university officer having responsibility for supervision of the information facility, or an authorised officer under schedule 1 of the Act, a user must -

- (a) obey a lawful direction given by the officer; or
- (b) produce suitable identification, including a student or staff card or a library borrower card.

5. Personal responsibility for QUT access account

(1) A user is responsible for any activity, transaction or publication of information which originates from their QUT access account.

(2) A user must not -

- (a) disclose any password or access code associated with their QUT access account to any other person;
- (b) allow any other person to use their account;
- (c) do any other act which may prejudice the security or integrity of their QUT access account.

(3) A user must accept responsibility for the use of their QUT access account prior to being granted access, or if requested to do so by the university from time to time.

6. Use of QUT access account

(1) A user must use their QUT access account for purposes related to university functions or activities.

(2) Despite sub-section (1), a user may use their QUT access account for incidental personal purposes provided that such use does not -

- (a) interfere with the functioning of information facilities systems or services; or
- (b) burden the university with excessive costs or exceed any quota imposed by the university for such use; or
- (c) in the case of a user who is an employee of the university, interfere with the user's employment.

(3) In this section, an "incidental personal purpose" does not include any of the following -

- (a) a purpose associated with a user's personal commercial interests, including advertising;
- (b) recruitment of members to, or soliciting donations for, political parties or religious groups;
- (c) the transmission, viewing or publication of pornography or other illicit or offensive material;
- (d) publication of internet sites or pages unrelated to university activities via the university's information facilities;
- (e) personal observations using inappropriate or offensive language published or transmitted via the university's information facilities;
- (f) a malicious or unlawful purpose.

7. Security of information facilities

(1) A user must comply with security measures for the protection of information facilities, including physical spaces and information technology networks, systems, services or data.

(2) A user must not do or attempt to do any of the following -

- (a) capturing or decoding any password or access code of another user;
- (b) circumventing any other security measures or access controls for the university's information technology systems or networks;
- (c) reading, capturing, copying, modifying or deleting data held in the university's information technology systems or networks without authority;
- (d) creating or installing any form of malicious software which may negatively affect the university's information technology systems, networks, software or data;
- (e) connecting or installing any device or software in the university's information technology systems or networks without authority.