College Network Acceptable Use Policy

Policy Number

CITG 004

Board approval:

Last amended: 2nd October 2012

Related policies:

Overview

The following policy sets out the requirements for the proper and responsible use of the CITG/College computing and network resources, effective protection of individual users, equitable access, and proper management of these resources. These guidelines are intended to supplement, not replace existing laws, regulations, agreements, policies, and contracts, which currently apply to these services.

Although the peer-to-peer file sharing is not prohibited, it can be used for the illegal downloading and distribution of audio, video, software and other files. Downloading or distributing material without permission of the copyright holder is a violation of federal and state law, even if it is not for profit. The penalties can be significant, including imprisonment and fines. Our refusal to censor access in no way condones violations of copyright or intellectual property laws.

With regards to peer-to-peer file sharing users should adhere to the "Three Ps" principal, of not sharing / downloading items that fall into the categories of:

- Plagiarism – copying of another person's work is a clear violation of university policy.
- Pornography – due to its size, the network is a broadcast medium, and as such the sharing of pornography is illegal.
- Piracy – sharing and copying of copyright material is illegal under federal legislation.

Copies of the current version of this and other IT related policies will remain available via the Resnet web site.

Policy

1. Acceptable Use

1.1. Users of ResNet are bound by the University of Queensland *Acceptable Use of UQ ICT Resources Policy*. This policy can currently be found at: https://ppl.app.uq.edu.au/content/6.20.01-acceptable-use-uq-ict-resources

1.2. ResNet users are additionally bound by the following rules and regulations intended to preserve the integrity and accessibility of all computing resources:

- Residential Computing network services and wiring may not be modified or extended beyond the area of their intended use. This applies to all network wiring, hardware and in-room data points.
- College data points may not be used to provide network access to anyone other than the resident assigned to the data point. Residents will be held responsible for all traffic generated by their assigned connection.
- Servers of any kind are prohibited without written authorisation from CITG. Individuals may use only the IP address assigned to them by CITG. Unauthorized use of a "fixed" IP address is prohibited.
- The residential network is a shared resource. Network uses or applications, which inhibit or interfere with the use of the network by others, are not permitted. Examples include but are not limited to file-sharing applications such as network game servers, and any excessive consumption of bandwidth.
- The residential network may only be used for legal purposes and to access only those systems, software and data for which the user is authorised. Sharing access to copyrighted material (including MP3 files from copyrighted music media and digitized video from copyrighted motion pictures, etc.) on the network is prohibited.
- Respecting the rights of other users, including their rights as set forth in other University policies for students, faculty, and staff, is required at all times on the network. These rights include but are not limited to privacy, freedom from harassment, and freedom of expression.
- Users are required to know and obey the specific policies established for the systems and networks they access.
- The residential network is provided for uses consistent with the academic mission of the institution. The network may not be used for commercial purposes nor for unsolicited advertising. Users may not provide open access to files/folders on their computers which contain anything that is protected by copyright (this includes MP3 files from copyrighted music media and digitized video from copyrighted motion pictures, etc.), or which would be in violation of the University's and/or community standards.
- Forgery or other misrepresentation of one's identity via electronic or any other form of communication is prohibited. Prosecution under State and Federal laws may also apply. This includes the use of an IP address not specifically assigned to the individual using it and the use of a forged or false identity.
- Any activity that can be deemed hostile such as port scans, email-bombs, ping-bombs, etc. are prohibited.

2. Non-Compliance

2.1. Use of ResNet constitutes FULL agreement and understanding of this Acceptable Use Policy and any future modifications there to. Violations of this policy may result in termination of connection, disciplinary sanctions, as well as legal sanctions. CITG Administrators have authority to control or refuse access to the network to anyone who violates these policies or who threatens the rights of other users. Administrators have the authority to suspend network access without notice for a user/computer that is believed to have been the source of an alleged violation pending investigation of the violation and satisfactory resolution of the complaint.

2.2. All complaints / infringements will be reported to the relevant college head who will institute their own disciplinary actions. An alleged breach shall be dealt with as follows:

- Initially, the resident shall be informed of the alleged breach, given an opportunity to respond to the allegation, and if it is not satisfactorily explained, a mandatory two week suspension from all CITG / College based computer facilities will be imposed.
- If when computing privileges are reinstated, the breach is not desisted from or remedied, the College may either permanently withdraw the resident's access to the computing facilities, or require the resident to show cause as to why they should be allowed continued residence.
- If the infringing conduct consists of a major breach of the University's Policies, then the College is also obliged to inform the relevant University authority

3. Underage Access

3.1. Legislation by the Federal Government restricts Internet services for people under 18 years of age. As colleges contain residents under the age of 18, this legislation is relevant to the use of the Colleges' network, and more specifically to the use of the pay-as-you-go Internet access. This legislation prohibits CITG from giving full Internet access to people under the age of 18 without written permission by a parent or guardian. Details of this legislation are available at the Australian Communications and Media Authority website.

3.2. By signing the **<insert name of college form here>** parents / guardians give permission for the student to have full access to the College Network and to the internet via the College Computer network. They agree that the College will not be held responsible for any content seen by the student.