

Broadcasting Services Amendment (Online Services) Act 1999

- UQ cannot provide Internet access to persons under the age of 18, unless written permission is given by a parent or guardian. This restriction applies to all systems allowing access to the Internet whether access is via centrally authenticated systems or via an organisational unit's own authentication system.
- ITS has implemented, and will continue to maintain, a system which tracks "under 18" students, together with an indication of whether parental permission has been received. This system uses the central directory and is linked to the central authentication system. It automatically prevents access to the Internet for "under W" students without permission, but only for access through the student Internet service linked to the central authentication system.
- If you allow students to have access to the Internet through your own authentication system, then you are responsible for ensuring that you have processes and systems in place to prevent access by "under W" students without appropriate permission.
- Under no circumstances is the University to host material that is (or would be) classified as RC or X. If R rated material must be hosted for University purposes, the Head of the Organisational Unit must give approval, and a Restricted Access System must be implemented and funded by the Organisational Unit. Minors are not to have access to these systems under any circumstances.
- The Director of ITS as the proper officer may take down any UQ hosted web site if directed by the Australian Broadcasting Authority.

COMPLIANCE DETAILS FOR BROADCASTING SERVICES AMENDMENT (ONLINE SERVICES) ACT 1999

The University of Queensland is an Internet Service Provider (ISP) and an Internet Content Host (ICH) and therefore has obligations under the Broadcasting Services Amendment (Online Services) Act 1999 (the Act).

In brief, the Act:

- Defines certain types of Internet content as prohibited content (or potential prohibited content).
- Provides for the approval by the Australian Broadcasting Authority (ABA) of industry codes of practice for ISPs/ICHs.
- Creates a mechanism through which members of the public may complain to the ABA about Internet content which they believe is, or may be, prohibited content.
- Empowers the ABA to investigate such complaints and, where appropriate issue notices to ISPs/ICHs to take action in relation to such content.
- Makes non-compliance with an ABA notice an offence, which attracts a significant financial penalty.

There are a number of Web references that will assist those who wish to have a more detailed understanding of the legislation and Codes. These are provided at the end of this document.

For the purposes of the Act, Internet content is defined as stored information that is accessible by an Internet carriage service. Types of Internet content that may be prohibited could include material on the World Wide Web, articles on newsgroups and bulletin boards and other information that can be downloaded from a library or archive of files.

Protection of Minors.

The University cannot provide Internet access to persons under the age of 18 years, unless written permission is given by a parent or guardian. There is an obligation to provide ABA sponsored material to parents to assist them in guiding the use of the Internet by minors and to advise parents of the procedure for reporting unsuitable content. The Director, ITS is responsible for ensuring that users of centrally provided university systems having access to the Internet, are identified and authenticated as permitted users. The Director, ITS will therefore be responsible for ensuring the provisions of the Act relating to minors are met by the University with regard to centrally authenticated systems.

If any organisational unit provides access to the Internet to students, without using the central authentication system, which automatically identifies under 18 students, that unit is responsible for implementing the provisions relating to protection of minors under the Act. The Director, ITS may bring to the attention of the ITSP any student Internet access facility where central authentication is not used.

Some areas of the University may, from time to time, have special programs for secondary students or research involving the participation of minors, where access to the Internet may form a part of such programs. The written

permission of a parent or guardian must be obtained before such access is provided. Forms and other material for this purpose are available from the ITS Service Centre.

Prohibited Content.

The following categories of Internet content are prohibited:

- Content which is (or would be) classified as RC (Refused Classification) or X by the Classification Board.
- Content hosted in Australia, which is (or would be) classified as R and which is subject to an ABA approved Restricted Access System (RAS) which is not applied. The RAS denies access to content by minors.

(References at the end of this document include web addresses for Classification Board Guidelines and the ABA Restricted Access System)

Under no circumstances is the University to host material that is (or would be) classified as RC or X.

No R rated content is to be hosted on University systems without the written approval of the Head of the organisational unit hosting the content. The Head is responsible for funding and implementing the approved ABA Restricted Access System.

It should be noted that the fact that a parent or guardian has permitted a minor to have access to the Internet does not remove the requirement that R rated material is not available to minors. Although this memorandum relates to online broadcasting legislation, there are other legislative requirements that protect minors from unsuitable material. The University Legal Officer should be consulted if there are any doubts about the suitability of material that might be accessed by minors.

Issue of Notices by the ABA.

For the purposes of the Act the University has nominated the Director ITS as the "Proper Officer" to receive notices from the ABA. If, after complaint investigation, the ABA is satisfied that content may be or is prohibited content, it will issue an interim or final or special take-down notice to the Proper Officer. The University must comply with such notices by 6pm on the next business day following receipt. Non-compliance with a notice is an offence under the Act and a separate offence for each day that it continues. The Director, ITS will have the authority to take down any content as directed by the ABA as the "Proper Officer" but will make every effort to discuss this with the organisational unit heads before action is taken.

Content Hosted Outside Australia.

The ABA approved Content Code 2 of the Internet Industry Code of Practice as the method of implementing Section 37 of the Act regarding RC and X content hosted outside of Australia. The ABA will adopt a Designated Notification Scheme that will notify suppliers of approved filters of prohibited or potentially prohibited content hosted outside Australia. The ABA will also advise ISPs of such content. ISPs have an obligation to make available to their users an approved filter or an alternative means of access prevention, at a charge determined by the ISP.

Where access to the Internet is via end-user facilities owned by the University, the Director ITS is responsible for implementing and managing procedures (preferably at the Internet/UQNET boundary rather than at each end user equipment) to meet the requirements of Code 2 without cost to other organisational units of the University.

Where access to University ISP services is from end-user equipment that is not owned by the University, the Director ITS is again responsible for meeting the requirements of the Act and the associated Code of Practice, but the Director may choose mechanisms that are appropriate to particular client groups. Staff and student dial-in accounts will not be required to meet additional charges.

IN SUMMARY

Key responsibilities as outlined in this document are summarised below:

DIRECTOR, ITS

- Responsible for ensuring the provisions of the Act relating to minors are met by the University, with regard to central authentication systems.

- The Director, ITS may bring to the attention of the ITSP any student Internet access facility where central authentication is not used.
- Director, ITS is the "Proper Officer" to ensure compliance of take-down notices issued by the ABA.
- The Director, ITS will have the authority to take down any content as directed by the ABA as the "Proper Officer", but will make every effort to discuss this with the organisational unit heads before action is taken.
- UQconnect provides relevant information to their clients on filters and access prevention.
- Relevant procedures are put in place on university systems to comply with the Act.

HEADS OF ORGANISATIONAL UNITS

- Where Internet access is provided to students without using the central authentication system, which automatically identifies under 18 students, the unit is responsible for implementing the provisions relating to protection of minors under the Act.
- If programs or research requires minors to access the Internet, permission forms must be signed by the minors' parent or guardian. Permission forms and other material can be obtained from the ITS Service Centre.
- RC or X rated material must not be hosted by University systems, under any circumstances.
- If R rated content is to be hosted on university systems, written approval is required from the Head of the organisational unit and the Head must provide funding for implementing an approved ABA Restricted Access System.

Web References:

Broadcasting Services Amendment (Online Services) Act 1999:

<http://scaleplus.law.gov.au/html/comact/10/6005/top.htm>

Classification Board Guidelines for the classification of films and videotapes: <http://www.oflc.gov.au/>

ABA criteria for restricted access system: <http://www.aba.gov.au/what/online>

ABA approved Internet Industry Association Codes of Practice: <http://www.iaa.net.au/>

ABA guidance to families: <http://www.cybersmartkids.com.au/>

University of Queensland Internet Code of Practice: <http://www.uq.edu.au/hupp> (see Section 6.10.1)

University of Queensland Network Management Policy: <http://www.uq.edu.au/hupp> (see Section 6.10.3)