

***ACCEPTABLE USE POLICY (INTERNET
AND NETWORK SERVICES)
(SCHOOLS AND NON-SCHOOL
MINISTRIES)***

POLICY 8



**St Francis Xavier Province of the
Christian Brothers
(Queensland and Northern Territory)**

MAY 2002

***EDMUND RICE EDUCATION DIRECTORATE
INDOOROOPILLY***

File Location: o:\education\luanne.cornhill\policies\internet.doc

1. INTRODUCTION

In line with technological development, Edmund Rice Schools/Ministries/Initiatives recognise the need to provide access to online services that enable young people to be taught and acquire knowledge and skills for the 21st Century. Such "services" include the Internet, Intranet and electronic mail.

2. SCOPE

This policy applies to all students/participants, staff and volunteers (User) of Edmund Rice Schools/Ministries/Initiatives.

Providing users with access to a vast amount of unfiltered information necessarily raises concerns that users will be exposed to ideas or material that may be unhealthy or, at the very least, non-educational or relevant to a ministry. Therefore it is highly appropriate for educational systems and employers to exert control over the use of the services they provide. Users must not access material where content would be inconsistent with the Mission Statement of the school and/or Edmund Rice Education. Nor must use of services be for purposes contrary to the law or Edmund Rice values.

The Acceptable Use Policy (AUP) is considered a tool to help educate all users about good citizenship in cyberspace.

3. PURPOSE

The purpose of this document is to provide Edmund Rice Schools/Ministries/Initiatives with a model policy and procedure, which will assist in establishing a consistent approach in respect of use of technology and issues of Internet and Network Services, provided by Edmund Rice Schools/Ministries/Initiatives. Such issues include establishing and maintaining an attitude of vigilance in relation to safety, misuse and legal liability. Failure to ensure safe and proper use of services by users expose others to harm and expose the Province to liability for that harm.

4. RATIONALE

Edmund Rice Schools/Ministries/Initiatives are guided not only by the common and statute law, but also those values which characterise the Reign of God as exemplified in the life and charism of our founder, Edmund Rice.

5. PRINCIPLES

It is expected that all users (employees, students/participants and volunteers) in Edmund Rice Schools/Ministries/Initiatives will, in the use of the services provided, refrain from any inappropriate use, uphold the policies of the school, the requirements of the law and guide their activities accordingly.

- Technological Services access is provided predominantly for an educational purpose and appropriate access will not be denied, restricted or suspended without due enquiry into problems and alleged violations.
- Xavier Province will not be responsible for financial obligations arising from unauthorised use of services provided.

6. ACCEPTABLE USE POLICY (AUP)

6.1 Students in schools and all other users may, subject to the following, have access to the Internet in order to achieve the maximum education or ministry opportunity.

6.2 Before being granted access to internet and email services, students in schools and their parent/guardian must sign an internet acceptable use agreement in the form which appears as Annexure A to this policy. A similar agreement for staff of Edmund Rice Schools/Ministries/Initiatives can be used and can be found in Annexure B.

- 6.3 Participants, staff and volunteers are to use the services for work related business and are directed to refrain from personal use of services provided beyond what is described as being **limited personal use**. Limited personal use means use that is infrequent and brief, e.g. use that occurs only a few times per day and for periods of a few minutes or less. Personal use should be restricted to breaks or outside usual hours. Participants, staff and volunteers using services for personal use must strictly adhere to this AUP at all times.
- 6.4 Users shall not access any objectionable or offensive material, material contrary to the law or material inappropriate to an educational or work environment. Examples of inappropriate use and inappropriate internet websites appear at Annexure B to this policy.
- 6.5 Users shall not post or forward defamatory, inaccurate, personal, sensitive, abusive, obscene, profane, sexually orientated, threatening, offensive or illegal material.
- 6.6 Email messages or attachments that contain, or are reasonably suspected to contain, offensive material must not be opened or sent.
- 6.7 Users must not personally subscribe to any External Mailing lists without the written approval of the Principal/Co-ordinator.
- 6.8 The network administrator may close an account at any time or as requested (e.g. by parent, Principal/Co-ordinator).
- 6.9 Users who suspect or know of inappropriate use must report to the Principal/Co-ordinator.
- 6.10 At the discretion of the Principal/Co-ordinator, any person identified as a security risk may be denied access to the services.
- 6.11 Any use of the internet by users which breaches this Policy, the Anti-Discrimination Act Queensland 1991 or other relevant laws, will result in disciplinary action against the user in accordance with the Christian Brother's Disciplinary Policies for staff or students. This action may include termination of employment for staff members, or expulsion for students.
- 6.12 Users should be aware that breach of this policy may also lead to external action being taken against them by a third party eg for breach of Anti-Discrimination laws or defamation.

7. ACCOUNTABILITY

- 7.1 Violations of this Policy will result in disciplinary action against the user.
- 7.2 Depending on the circumstances, internal penalties for violation of ethical use and acceptable use of services will include:
- suspension or revocation of an account;
 - suspension of the user's access to the service;
 - implementation of the school/ministry/initiative disciplinary procedure for students;
 - implementation of the Staff Disciplinary Policy;
 - archiving of user data as part of record; and/or
 - provision of relevant records to State or Commonwealth authorities for the purposes of lawful investigations.

8. RESPONSIBILITIES

- 8.1 The accountabilities of ERED include:
- the establishment of Policy and Procedure setting out reasonable boundaries in relation to what is considered acceptable use of services provided; and
 - reviewing any development of school/ministry/initiative policies in line with this Policy.

8.2 Accountabilities of Principal/Co-ordinator/Delegate include:

- apply AUP to school/ministry/initiative use;
- ensure all staff/volunteers receive instruction in AUP;
- ensure all students/participants are aware of AUP;
- establish a process to ensure adequate supervision in schools of students using the services;
- establish procedures for conducting school activities, such as website, page site creation; and
- maintain school user agreements in consultation with students, parents and guardians.

8.3 Responsibility of staff/volunteers :

- all staff/volunteers are bound by the AUP for their own use and share supervisory responsibility for students/participants using the services; and
- should a staff/volunteers become aware of unacceptable use by other staff/volunteers, it must be referred immediately to the Principal/Co-ordinator.

8.4 Responsibility of parents :

- address with their students/participants any additional boundaries as to what they consider acceptable use.

8.5 Students/Participants

All students/participants and parents/guardians are to sign an Acceptable Use Agreement prior to the student/participant going online and students are expected to comply with the AUP at all times.

9. PRIVACY—ALL USERS

9.1 Good systems administration includes regular backups and the monitoring of logs reflecting all use of the systems. Normal systems administration may have the effect of collecting information provided by the user including email messages, both active and deleted, as well as internet sites visited. The right is reserved to monitor user activity to ensure adherence to the principles of this document and then to act as deemed appropriate. Individualised searches will be conducted if there is a reasonable suspicion that a user has violated the law or school rules.

9.2 All users are directed not to display personal/sensitive information about another person on the net without that person's permission.

9.3 Users are directed not to publish identifying information about children or photographs of children on the internet without consent.

9.4 The Privacy Amendment (Private Sector) Act 2000 (Commonwealth) applies to private educational institutions and establishes 10 National Privacy Principles and must be complied with by Edmund Rice Schools/Ministries/Initiatives. (Please refer to Province Privacy Policy.)

9.5 All attempts should be made to keep information secure. A common means of gaining illegal access to electronic information is to break a legitimate users password. Staff/volunteers should select passwords that are not easy to guess or to find using a password-breaking program. Passwords need to be changed regularly.

**ANNEXURE A
INTERNET ACCEPTABLE USE AGREEMENT
STUDENT / PARTICIPANT**

For the use of School/Ministry/Initiative Learning Technology Resources

This section must be completed by the student/participant.

Before you may use computer facilities at {School/Ministry/Initiative Name}, you must sign this contract which binds you to the following conditions. If you break any of the conditions, appropriate penalties will be applied.

Your Name: Year Level:

Network Login Name: Ministry:

I have read the Policy and Guidelines for Acceptable Use of Internet and Network Resources and agree to obey the guidelines and conditions in it and take responsibility for my actions. I understand that the school/ministry/initiative shall not be responsible for the consequences of any misuse of the internet, intranet or electronic mail by me.

Signed: Date:
Student

This section must be completed by the parent or legal guardian of the student/participant.

I, the parent or guardian of have read and understood the *Acceptable Use of Internet and Network Services Policy* document. I agree that my child is permitted to use the school/ministry/initiative internet, intranet or electronic mail and that he/she is aware of the obligation to observe these guidelines and conditions and to be responsible for acceptable use. I understand that the school/ministry/initiative shall not be responsible for the consequences of any misuse by my child.

Signed: Date:
Parent/Guardian

**ANNEXURE B
INTERNET ACCEPTABLE USE AGREEMENT
STAFF / VOLUNTEERS**

For the use of School/Ministry/Initiative Learning Technology Resources

This section must be completed by the staff member/volunteer.

The employer extends to staff/volunteers the opportunity to use technology resources. Before you may use computer facilities at {School/Ministry/Initiative Name}, you must sign this contract which binds you to the following conditions. If you break any of the conditions, appropriate penalties will be applied.

Your Name: **Position:**

Network Login Name: **Ministry:**

I have read the Policy and Guidelines for Acceptable Use of Internet and Network Resources and agree to obey the guidelines and conditions in it and take responsibility for my actions. I understand that the school/ministry/initiative shall not be responsible for the consequences of any misuse of the internet, intranet or electronic mail by me.

Signed: **Date:**
Staff Member / Volunteer

ANNEXURE C ALL USERS

INAPPROPRIATE USE

The use of the intranet, internet and email must not be used to:

1. infringe the copyright or other intellectual property rights of third parties, for example, staff should not download and use work without the express permission of the owner;
2. download software, unless appropriate authorisation and compliance with licensing requirements and established policies to check all such software for computer viruses is followed;
3. disrupt communication and information devices through such means as mass emailing or transmitting files which place an unnecessary burden on departmental resources;
4. access inappropriate internet sites (see below);
5. download, distribute, store or display offensive or pornographic graphics, adult sites, images or statements or other material obtained from inappropriate internet sites;
6. access material that is discriminatory or could cause offence to others, for example, offensive material based on gender, ethnicity or religious or political beliefs;
7. download unreasonable amounts of material for non-work related or non-educational use;
8. download information for the purpose of providing it to external organisations or the general public without authorisation;
9. distribute chain letters;
10. distribute defamatory, obscene, offensive or harassing messages;
11. distribute confidential information without authority;
12. distribute messages that disclose personal/sensitive information without authorisation;
13. distribute private information about other people;
14. distribute messages anonymously, using a false identity or using another person's email account;
15. engage in any illegal or wrongful activity; and
16. download/supply to others inappropriate site addresses.
17. Knowingly engaging in any activity which may compromise the security of the local area network, intranet or external network.

INAPPROPRIATE INTERNET SITES

Inappropriate sites include, but are not limited to, sites that:

- a) are illegal;
- b) are pornographic or contain inappropriate or obscene sexual material;
- c) advocate hate/violence;
- d) contain discriminatory material, e.g. on the basis of gender, race, religious or political beliefs; and
- e) offer inappropriate games or software.