EDMUND RICE EDUCATION
AUSTRALIA

ACCEPTABLE USE POLICY INFORMATION COMMUNICATION TECHNOLOGY

INCLUDING

INTERNET AND NETWORK SERVICES

IN SCHOOLS AND NON-SCHOOL MINISTRIES

Policy 8

JANUARY 2013

1. INTRODUCTION

In line with technological development, Edmund Rice Education Australia (EREA) Schools 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 all Information Communication Technology (ICT) and is not limited to the Internet, Intranet and electronic mail.

Definition:

In this policy document the term School(s) refers to and includes EREA Schools, Colleges, Flexible Learning Centres, Indooroopilly Montessori Children's House or any other EREA ministry within the Northern Region.

2. POLICY STATEMENT

EREA is committed to the provision of safe access to Information Computer Technologies for all employees and Students to support the teaching learning program and administration of Schools.

3. SCOPE

This policy applies to all users of ICT - students, staff and volunteers in EREA Schools.

It applies to all ICT, devices, connections and networks used and accessed at school whether school owned or owned by students, staff or volunteers and all school owned devices and networks used and/or accessed at school or elsewhere.

For the sake of clarity, the words "staff" and "employees" include persons employed by EREA (Trustees of the Christian Brothers Queensland and/or Oceania) on a full-time, part-time, temporary, permanent, contractual, casual basis or through an agency and includes student teachers and any other adults who in the course of their duties have access to school or EREA owned or administered ICT including access from a home connection.

4. PURPOSE

The purpose of this document is to provide EREA Schools with a policy and procedure, which will assist in establishing a consistent approach in respect of use of ICT and issues of Internet and Network Services, provided by EREA Schools.

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 may expose others to harm and therefore may expose EREA to liability for that harm.

5. RATIONALE

EREA Schools 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. Users must not access material where content would be inconsistent with the Mission Statement of the school and/or Edmund Rice Education Australia. Nor must use of services be for purposes contrary to the law or the values in the EREA Charter.

Users in EREA schools are provided with access to selected ICT including Internet and Intranet facilities and services to support their roles in teaching and learning, research and administration. Access to these services and facilities is intended to facilitate increased learning opportunities for school personnel within the framework of the purpose and mission of EREA through the provision of information, and enhanced opportunities for communication and collaboration.

Use for other non-educational reasons, including but not limited to, conducting business or commercial activity, other profit making ventures, product advertising, disclosure of personal, private or EREA information, political activity and mischievous or fraudulent purposes, is not acceptable and may be dealt with under EREA policies, or State or Commonwealth law as applicable

6. PRINCIPLES

It is expected that all users (employees, students/participants and volunteers) in EREA Schools 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.

1. All users of ICT in EREA - Schools must act with respect and integrity.
2. ICT 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.
3. Safe learning and work environments will be provided for all students, employees, parents and volunteers.
4. Users must demonstrate respect for intellectual property, ownership of data and information, system security, mechanisms and the individual's right to privacy. They need to deal with material in which intellectual and industrial property rights may subsist in law including the law of copyright, registered designs, trademarks and patents.

7. ACCEPTABLE USE POLICY

7.1. For Students

7.1.1. Students should respect resources

7.1.1.1. Use ICT equipment and resources for educational purposes independently and under staff supervision

7.1.1.2. Follow staff directions for accessing files, programs, emails and internet resources

7.1.1.3. Delete emails from unknown sources without opening any attachments as they may contain viruses

7.1.2. Students should respect others

7.1.2.1. Respect the rights, beliefs and viewpoints of others

7.1.2.2. Follow the same standard of behaviour online as one is expected to follow generally

7.1.2.3. Observe copyright rules

7.1.3. Students should keep themselves safe online

7.1.3.1. Keep passwords and personal work secure

7.1.3.2. Use the internet and email for educational purposes

7.1.3.3. Use school email accounts, not personal email accounts, when communicating online at school

7.2. For Staff acceptable use of ICT includes the following

7.2.1. Facilitating, gathering and disseminating appropriate information

7.2.2. Encouraging collaborative projects and resource sharing

7.2.3. Fostering innovation

7.2.4. Fostering professional learning

7.2.5. Undertaking administrative functions that support the employer

7.2.6. Well considered and efficient use of resources

7.2.7. Work related use which includes (but is not limited to) the following

7.2.7.1. Curriculum related information and resources

7.2.7.2. Student welfare and pastoral issues

7.2.7.3. Professional and educational issues

7.2.7.4. Communicating with work colleagues

7.2.7.5. Employment related information such as access to policies

7.3. Before being granted access to ICT, internet and email services, users including staff, students in schools and their parent/guardian must sign an Internet Acceptable Use Agreement in the form similar to those which appears as samples in Annexure A or Annexure B (as appropriate) to this policy. Annexure C provides a brief summary of unacceptable use.

7.4. Users are accountable for a duty of care in terms of the information they provide and access over Internet/Intranet connections;

7.5. Schools and authorised users connecting to the internet and intranet will be accountable for the ethical and appropriate use of information and networks;

7.6. Every effort is to be made to use any information services provided in a cost-efficient way;

7.7. Users are to adhere to considered and appropriate records management practices.

7.8. Email messages or attachments that contain, or are reasonably suspected to contain, offensive material must not be opened or sent

7.9. The network administrator may close an account at any time or as directed by the, Principal/Co-ordinator.

7.10. Users who suspect or know of inappropriate use must report such as suspicion to the Principal/Co-ordinator.

7.11. At the discretion of the Principal/Co-ordinator, any person identified as a security risk may be denied access to the services.

7.12. 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 EREA's Disciplinary Policies for staff or students. This action may include termination of employment for staff members, or expulsion for students.

7.13. 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.

7.14. All users must use the secure password and not divulge it to others. If it is believed that a password has been compromised or an account used by others, steps must be taken to change the password and/or account immediately including immediate advice to the Principal/Coordinator.

8. UNACCEPTABLE USE

8.1 All users may, subject to the following, have access to the Internet in order to achieve the maximum education or ministry opportunity.

8.2 Users may 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 Acceptable Use Policy all times. All use of ICT provided by EREA or Schools may be recorded, monitored and audited. Such monitoring or auditing may disclose internet sites visited and email messages both active and deleted. Content stored on ICT equipment is the property of EREA, may be viewed by authorised staff within EREA and is 'discoverable documents' that may be subpoenaed in relation to court proceedings and may be required to be disclosed..

8.3 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.

8.4 Users shall not post or forward defamatory, inaccurate, personal, sensitive, abusive, obscene, profane, sexually orientated, threatening, offensive or illegal material.

8.5 Users must not personally subscribe to any External Mailing lists without the written approval of the Principal/Co-ordinator.

8.6 Users must not share the use of accounts.

8.7 Users must not attempt to gain access to systems or services without authorisation, or engage in activities which disrupt or corrupt services or information;

8.8 Users must not disclose personal information of school personnel or group email addresses to agencies or individuals outside EREA;

8.9 Users must not access, intercept, modify or destroy email, data, files or programs belonging to other users or engage in activities which harass or threaten other users;

8.10 Users must not access, download or distribute copyrighted or illegal material or material of a morally dubious nature from the Internet. Employees must respect any Intellectual Property right or interest which has previously arisen or may arise in the future in subject matter created, developed or otherwise coming into existence in the course of, relating to or as a result of his/her employment within an EREA School including but not limited to subject matter that gives rise to issues concerning Copyright, Trade Marks, Designs, Patents, will remain the property of and vests absolutely and exclusively with EREA or its Schools. Employees must give EREA or the EREA School full details of such subject matter.

8.11 EREA will not be responsible for financial obligations arising from unauthorised use of services provided.

8.12 Staff may not use ICT social networks such as but not limited to Facebook, MySpace, Twitter or YouTube to contact, access or engage with students presently enrolled in any school. (An exemption to this contact on internet social networks exists for an employee for contact with students who are part of his/her immediate family or accessing sites created and maintained by a member of the employees immediate family and for any EREA or school formally authorised and administered site)

8.13 EREA employees shall observe the requirements of the Privacy Act (1988) as amended. All staff must take responsibility for the security of the ICT provided for their use, not allowing them to be used by unauthorised persons or in an unauthorised manner.

8.14 All staff are required to observe the provisions of the Privacy Act, especially when dealing with confidential, private or sensitive information.

8.15 All staff must ensure that they do not use or disclose confidential information for a purpose other than carrying out their duties.

8.16 This Code of Practice is written in accordance with the national privacy principles and the national privacy commissioner's guidelines*

> *"While staff are given a password which allows access to their files, e-mail account and web browsing, system administrators are technically able to access everything on the network. Most e-mails are insecure unless it is encoded or encrypted. E-mails are hard to destroy. Most electronic documents are backed up and recoverable Software used to operate network logs, transactions and communications. E-mail logs normally include the addresses of senders and recipients and the time of transmission. Web server logs record information on the sites that people visit."* www.privacy.gov.com

8.17 All school and EREA e-mail must contain a disclaimer, for example:

> *"The information contained in the above e-mail message or messages which includes any attachment, is confidential and may be legally privileged. It is intended only for the use of the person or entity to which it is addressed. If you are not the addressee, any form of disclosure, copying, modification, distribution or any action taken or omitted in reliance on the information is unauthorised. Opinions contained in the message(s) do not necessarily reflect the opinions of EREA or (Name theSchool). If you received this e-mail message in error, please immediately notify the sender and delete the message from your computer."*

9. ACCOUNTABILITY

9.1. EREA strives to cooperate with other systems administrators, network providers, legal authorities of the State and Commonwealth and the international community to provide a reliable and trustworthy service.

9.2. Violations of this Policy will result in disciplinary action against the user. The EREA response to proven unethical or unacceptable use of these services depends on the severity of the breach. This response may include implementation of the school/ministry/initiative disciplinary procedure for students, implementation of the Staff Disciplinary Policy including continuing employment considerations, suspension of access privileges, archiving of user data as part of EREA records.

9.3. Giving access to appropriate records to State or Commonwealth authorities for the purposes of their lawful investigations may also be considered.

9.4. The user, by accessing and using EREA's ICT, email, intranet and internet facilities and by entering personal information into the system, consents to the use or disclosure of that information by EREA.

9.5. EREA will not in any circumstance be responsible for any incidental or consequential damages of any nature or kind whatsoever incurred in or as a result of the use of this service, including but not limited to damages arising from a breach of the conditions in sections 6 and7. EREA does not guarantee the quality or accuracy of Internet information. Users are responsible for evaluating the validity and integrity of Internet information.

10. RESPONSIBILITIES

10.1 The accountabilities of EREA 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.

10.2Accountabilities of Principal/Co-ordinator/Delegate include:

- apply the Acceptable Use Policy (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 staff, students, parents and guardians.

10.3Responsibility of staff/volunteers :

- all staff/volunteers are bound by the Acceptable Use Policy 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.

10.4Responsibility of parents :

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

10.5Students/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.

11. PRIVACY—ALL USERS

11.1. 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.

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

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

11.4. 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. (Please refer to Province Privacy Policy.)

11.5. 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

1. Introduction

The purpose of Information and Communication Technologies (ICT) at <….insert school name here….> is to:

- enhance student learning opportunities
- promote student achievement
- enhance the school's management information and business administration systems
- <…schools add more here if required….>

The use of ICT within the school should be responsible, legal, appropriate and for educational purposes and should follow the guidelines outlined in this Code of Practice.

This Code of Practice applies to the use of all school related ICT whether provided by the school, employees of the school or the student.

Both students and parents/guardians must read and sign this Code of Practice. It should be returned to <…insert school details here…>

2. Definitions

Information and Communication Technologies (ICT) is any electronic device or related applications which allow users to record, send, access or receive information, in textual, audio, image or video form. These may include but are not restricted to:

- computer systems and related applications such as email and internet
- web-based tools such as discussion forums, chat rooms, blogs, podcasts, internet social networks and instant messaging systems
- mobile devices such as mobile phones, PDAs
- fax machines, scanners
- output devices such as printers
- imaging tools such as video or still cameras
- audio tools such as audio recording devices
- <…schools add more here if required….>

3. Acceptable Uses

3.1 Students should

- Respect resources
- Use ICT equipment and resources for educational purposes independently and under staff supervision
- Follow staff directions for accessing files, programs, email and internet resources
- Delete emails from unknown sources without opening any attachments, as they may contain a virus

3.2 Respect others

- Respect the rights, beliefs and viewpoints of others
- Follow the same standards of behaviour online as one is expected to follow in real life
- Observe Copyright rules by respecting the information, ideas and artistic works of others by acknowledging the author or publisher of information from the internet and not claiming the work or pictures as your own

3.3 Keep yourself safe online at school

- Keep passwords and personal work secure. If it is suspected that a password has been compromised, steps must be taken to change the password immediately.
- Use the internet and email for educational purposes
- Use school email accounts, not personal accounts, when communicating online at school

4. Unacceptable Uses

4.1 Personal Safety

Disclosure of personal information can expose users to inappropriate material, physical danger, unsolicited commercial material, financial risks, harassment and bullying, exploitation, unreliable information, nuisance and sabotage.

You should NOT:

- Send or post detailed personal information, images or audio about yourself or other people. Personal contact information includes home address, telephone or mobile number, school address or work address.
- Publish email addresses to public sites
- Meet with someone you have met online without your parent's/guardian's approval and participation
- <…schools add more here if required….>

4.2 Illegal Activities

Students need to be aware that they are subject to laws including those governing assault, trafficking and computer offences. An electronic audit trail may provide evidence of offences.

You should NOT

- Attempt to gain access to any computer system or service, to which you do not have authorised access. This includes attempting to log in through another person's account or accessing another person's files or emails.
- Make deliberate attempts to disrupt other people's use of ICT
- Make deliberate attempts to destroy data by hacking, spreading computer viruses or by any other means
- Engage in any illegal acts
- Install or use software which is not licensed by the school
- <…schools add more here if required….>

4.3 Network Security

You should NOT:

- Provide your password to another person
- Go looking for network security access, because this may be seen as an attempt to gain unauthorised access to the network
- Post information that, if acted upon, could cause damage to or disrupt the network
- Open e-mails from unknown sources
- <…schools add more here if required….>

4.4 Inappropriate Language

Restrictions against 'inappropriate language' apply to public messages, private messages, and material posted on web pages. Messages sent using the school's ICT are recorded, monitored and scanned.

You should NOT:

- Use obscene, profane, rude, threatening, sexist, racist, disrespectful or inappropriate language
- <…schools add more here if required….>

4.5 Respect for Privacy

You should NOT:

- Distribute private information, including email, photos or recordings, about another person without their permission
- Take photos, sound or video recordings of people, including background figures and voices, without their permission

- <…schools add more here if required….>

4.6 Respect for Others

You should NOT:

- Make personal attacks on another person
- Harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If someone tells you to stop sending them messages, you must comply with their request.
- Send or post any inappropriate or inaccurate information, comments, images, video or audio about other people, the school or other organisations
- Send or post personal information about other people without their permission
- <…schools add more here if required….>

4.7 Respecting Resource Limits

You should NOT:

- Download or send large files (>5 Mb) without teacher permission
- Post or respond to chain letters or engage in 'spamming'. Spamming is sending an annoying or unnecessary message to a large number of people.
- <…schools add more here if required….>

4.8 Plagiarism and Copyright

You should NOT:

- Plagiarise works found on the internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- Use material from the internet in a manner which violates copyright laws
- Access or use material from the internet which relates to exam cheating or providing completed assignments
- <…schools add more here if required….>

4.9 Access to Inappropriate Material

Attempts to access inappropriate material using the school's ICT is monitored and logged by the school.
Some inappropriate material may be filtered or blocked by the school.

You should NOT:

- Use ICT to access material that:
- is profane or obscene (pornography)
- advocates illegal acts
- advocates violence or discrimination towards other people
- Participate in internet social networks, online chats, discussion groups or mailing lists that are not relevant to your education
- Access material which is not relevant to your education
- Use the school ICT to purchase, order or sell any goods
- <…schools add more here if required….>

5. Notification

You should:

- Disclose to your teacher any messages you receive that are inappropriate or disturb you
- Notify your teacher if you identify a possible security problem
- Immediately disclose accidental access to inappropriate material to your teacher. This will protect you against an allegation that you have intentionally violated the School's ICT Code of Practice.
- Notify your teacher if you are offended by another person's use of ICT.

6. Consequences of Improper Use

Any user violation will be recorded and may be subject to the following consequences:

- loss of access privileges for a period of time
- informing parents/guardians
- suspension or termination of enrolment
- legal action
- payment for damage to equipment/resources
- <….schools add more here if required….>

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: ....

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

Annexure C is to be included with Annexures A, and B

INAPPROPRIATE USE INCLUDES BUT IS NOT LIMITED TO THE FOLLOWING

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. 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

offer inappropriate games or software.