VALUES

Equity, Trust, Respect.

POLICY

Saint Clare’s School seeks to provide an educational environment which will enhance academic learning opportunities, for all students, through the integrated and equitable use of available information and communication technologies as described by the Diocese.

GUIDELINES

1.1 It is recognised that information and communication technology (ICT) has the ability to enhance learning in all areas of the curriculum.

1.2 The school will, as financial resources allow, provide ICT systems for use by students and staff for education and research.

1.3 Undesirable or inappropriate material is not to be used and inappropriate use of the School's systems will result in disciplinary action.

1.4 Students will be supervised at all times when accessing the internet. Students also have an obligation to follow teacher directions and only access approved material.

1.5 The School will from time to time be placing photographic images of staff and students on the School website and in other publications.

1.6 If a Saint Clare’s community member does not wish their image or personal information to appear on the website or in any School publication, they should inform the School in writing.
ACCEPTABLE USE GUIDELINES

1. Use of ICT systems

1.1 The use of ICT systems must be in support of education and research and be consistent with the educational objectives.

1.2 Use of other organisation’s networks or computing resources must comply with the rules appropriate for that network.

1.3 Transmission/Downloading of any material in violation of any Australian law is prohibited. This includes but is not limited to:
   - copyrighted material
   - threatening or obscene material

1.4 Undesirable or inappropriate material is not to be used or downloaded.

2 PRIVILEGES

2.1 The use of St Clare’s School ICT systems is a privilege, not a right, and inappropriate use may result in the withdrawal of this privilege and a renegotiation of the users privileges.

2.2 Before gaining access to the Internet, each user will be required to read and sign an ICT user agreement. Users will then undergo training in the proper use of the internet.

2.3 The administration and staff of St Clare’s School may request the system administrator to deny, revoke or suspend specific user access.

3 NETWORK ETIQUETTE

3.1 Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

   (i) Privacy Not revealing personal addresses or telephone numbers of self, other students or colleagues.

   (ii) Appropriate language Not using inappropriate language.

   (iii) Politeness Not writing or sending abusive messages to others.

   (iv) Fairness Not using the network in such a way as to disrupt the use of the network by other users, such as downloading very large files during prime time, sending e-mail messages to multiple addresses, use which annoys other users, etc.

Note: While it is not the intent to read private correspondence, electronic mail (e-mail) is not guaranteed to be private. People who operate the system have access to all mail. Messages relating to or in
support of illegal activities may be reported to the authorities.

4 STUDENT USE

4.1 Normally student use will be during school hours. Student use outside of school hours will be only by arrangement with the supervising teacher.

5 SECURITY

5.1 Security on any computer system is a high priority, especially when the system involves many users. These practices must be followed:

(i) Users who can identify a security problem must notify a staff member or the system administrator. They must not demonstrate the problem to other users.

(ii) A user who has a password must not disclose it to any other individual.

(iii) Users may access only their own accounts.

(iv) Attempts to log into the system by impersonation will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems will be denied access.

6 VANDALISM

6.1 Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy

1. data found on the network
2. computer software
3. hardware
4. by spreading of computer viruses

APPROVED: 2011 REVIEW: 2014