COMPUTER AND INTERNET ACCESS POLICY

The Internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Online communication links students to provide a collaborative learning environment and is intended to assist with learning outcomes. Students are exposed to online communication tools and the internet in their community. They have the right to expect secure access to these services as part of their learning experiences at St Mark's Anglican Community School.

1.0 PURPOSE

This Policy is designed to establish clear guidelines about the responsible use of the internet and online communication services provided by the School. The responsible use of these services by students, with guidance from teaching Staff, will provide a secure and safe learning environment. To use these services, each student and Staff member must agree to abide by the School's policy.

2.0 COVERAGE

2.1 This Policy applies to everyone who is:

(a) employed by St Mark's Anglican Community School

(b) in a teaching, practicum or management position or role at the School

(c) a student who accesses internet and online communication services with the School and from any external location.

2.2 This policy covers the use of School computers and other electronic devices including internet access, email protocols, electronic records access, security of information and confidentiality.

2.3 This policy document should be read as consistent with the Pastoral Care, Managing Behaviours, and Social Networking and Intellectual Property policies.

3.0 POLICY

3.1 The use of the internet and online communication services provided by St Mark's Anglican Community School is intended for research and learning between Staff and students. Access to internet and online communication tools at school will assist students to develop the information and communication skills necessary to use the internet effectively and appropriately.

3.2 Staff use these services for lesson preparation, record keeping, accessing the internet, sending emails and any other purpose related to carrying out their duties as employees of the school.

3.3 Students are able to gain access to the School's Internet System by completing an Internet Access Form. This form must be signed by both parents/guardians, where possible.

3.4 Deliberate attempts to seek or use material that is illegal or which would be regarded by reasonable persons as offensive is not permitted.

3.5 The School Administration has the final say in deciding what is or is not offensive in the school context but will be guided by the Commonwealth Crimes Act which states that a person shall not knowingly or recklessly: *Use telecommunication services supplied by a carrier in such a way as would be regarded by reasonable persons, as being in all circumstances, offensive.*

3.6 Use of the Internet in an offensive manner can result in a criminal investigation.

3.7 The School owns all messages and transmissions conducted through its system and therefore are legally responsible for all messages and transmissions.

4.0 RESPONSIBILITIES

4.1 The responsibility for setting up and conveying standards and dealing with inappropriate material is a joint responsibility with Staff, students, families and School. Internet and email access is a privilege; not a right as access involves responsibility.

4.2 The School will support students in safe, appropriate internet use. This support includes: regular web page screenings, Internet filters

4.3 Staff using internet and online communication services have the responsibility to report inappropriate behaviour and material to the Principal, Head of ICT and/or Head of School.

4.4 Students using internet and online communication services have the responsibility to report inappropriate behaviour and material to the supervising teacher, Head of ICT and/or Head of Department.

4.5 The Network Manager and Computer Technicians have the responsibility to report inappropriate material found on Staff and students' laptops to the Head of School and the Principal.

4.6 Staff and students who use the internet and online communication services provided by the School must abide by the School's conditions of acceptable usage.

4.7 Computer systems at the School are protected by password access as well as physical barriers. At no time should third parties be given unsupervised access to School records.

5.0 STUDENT ACCESS

5.1 Only software purchased or approved by the School, and installed by the School, can be used on School equipment. It is illegal to copy copyrighted software contrary to the School's Licence Agreement.

5.2 No software or data on the School computer system may be copied.

5.3 Printing from CD-ROM or downloading and printing from the Internet is permissible for the purpose of school related study and research.

5.4 Abuse or deliberate misuse of computer equipment will result in disciplinary measures determined by the Head of Year and Head of School. This could

include being banned from using all school electronic facilities for a specified time.

5.5 Any external disk must be scanned for viruses prior to being used on any School computer.

5.6 All internet accesses are logged. Although records of usage are not monitored on a systematic basis, nor are random checks undertaken, should an issue arise in relation to email and internet usage, the relevant records would be accessed.

5.7 If students are found misusing their access to the Internet or email by sending abusive letters or accessing offensive material that will be referred to the Head of School for disciplinary action and access to the network will be denied for a period of time specified by the Principal or Head of School.

5.8 Students are to respect the privacy and ownership of others' work at all times. This includes not plagiarising downloaded information and presenting it as their own work or copying work of other students.

5.9 Settings for virus protection, spam and filtering must not be disabled.

5.10 Students must not seek out inappropriate material. This includes racist, pornographic, irreligious or material with obscene language. This also includes sexually explicit or sexually suggestive material or correspondence.

5.11 Students are to log off at the end of each session to ensure that nobody else can use their e-learning account.

6.0 STAFF ACCESS

6.1 Only software purchased or approved by the School, and installed by the School, can be used on School equipment. It is illegal to copy copyrighted software contrary to the School's Licence Agreement.

6.2 Software copying must be in accordance with legal requirements, and 'pirate' software is not permitted on any school owned computer.

6.3 Printing from CD-ROM or downloading and printing from the Internet is permissible for the purpose of school related study and research.

6.4 Deliberate attempts to seek, use or transmit material that is illegal or which would be regarded by reasonable persons as offensive is not permitted.

6.5 Staff should ensure that confidential documents or records are not left on desktops to be viewed by third parties.

6.6 All internet accesses are logged. Although records of usage are not monitored on a systematic basis, nor are random checks undertaken, should an issue arise in relation to email and internet usage, the relevant records would be accessed.

6.7 Staff should be aware that email harassment and/or technology harassment can occur on any grounds of discrimination. The School will not tolerate email/or internet harassment. Any issue involving harassment or discrimination could result in disciplinary action.

6.8 Staff are required to maintain confidentiality with reference to student and family records and information. Where appropriate, the School will ensure the privacy of Staff, student and family records through restricted access to records by relevant Staff responsible for maintaining such information.

7.0 NETWORK POLICY

7.1 The School attempts to prevent and/or detect viruses by ensuring suitable virus detection software is maintained on computer networks within the School.

7.2 No shareware type external games disks should be used in a School computer.

7.3 Users do not have permission to utilise a public Social Network on a School computer such as MSN, Facebook etc. (Refer to the Social Networking Policy)

7.4 All email messages should have the following Disclaimer included below signature: *This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please inform the sender and delete it from your mailbox or any other storage mechanism.St Mark's Anglican Community School accepts no liability for any statements made which are clearly the sender's own and not expressly made by an authorized representative of St Mark's.*

7.5 If a virus is detected on computers, contact the Network Manager or Computer technicians for it to be removed.

7.6 As a matter of protocols, all email attachments are checked automatically by virus protection software. If there is an uncertainty about a file, the Computer Technicians must be notified. Any files that end with .COM or .EXE should be first saved to hard disk and then scanned for viruses. If the source of the email is not known it would probably be erased.

7.7 The use of email for personal communication is permitted within reasonable limits. Email facilities cannot be used for any individual commercial activities.

7.8 Individual Staff members are responsible for the regular checking of their email messages. Staff should make arrangements for the checking of their email during any periods of leave.

7.9 All email messages should be actioned. Email will work more efficiently if not clogged up with unwanted emails. Create new folders to keep wanted emails safe and ordered.

7.10 As with all documents, Staff should ensure that copyright provisions are followed in relation to materials sent by email.