Computer Use Policy

PURPOSE OF THE POLICY

The purpose of this policy is to outline guidelines for computer use, and for the security and confidentiality of electronic information at (AIIC).

Scope
The policy applies to all staff, students and other users of the school electronic communication facilities and covers the use of school computers and other electronic devices, including internet access, email protocols, electronic records access, and security of information and confidentiality requirements.

Responsibility
Principal

Point of Contact
IT Coordinator

POLICY

(AIIC)provides students and staff with computer facilities for educational use. The resources provided include computers, printers, interactive whiteboards, data projectors, CD-ROM access and access to email and the internet.

Students may use these facilities for educational and research purposes only, including for class work, for the preparation of assignments and for the development in skills using a computer.

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

To use these resources, each student and staff member must agree to abide by the school's policy.

Students

Students are able to gain access to the school's Internet system by completing an Internet access form. The form must be signed by both parents, where possible, and the student. Students should be aware that in signing the form for computer access, they are agreeing to the following:

- 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 License Agreement. No software or data on the school computer system may be copied. Printing from CD-ROM or downloading and printing from the internet is allowed for the

purpose of school related study and research. Abuse or deliberate misuse of computer equipment will result in discipline by the Principal and may include being banned from using all school electronic facilities for up to one term.

- Deliberate attempts to seek or use material that is illegal or which would be regarded by reasonable persons as offensive is not permitted. The school administration has the final say in deciding what is or is not offensive in the school context, but will be guided by Section 85ZE of 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.' **Use of the Internet in an offensive manner can result in criminal prosecution**.
- Students should be aware that all internet accesses are logged.
- If students are found misusing their access to the Internet or email by, for example, sending chain letters or abusive letters or accessing offensive material they will be referred for disciplinary action and access to the network will be denied for a period specified by the Principal or the Principal's nominee.
- The school is particularly concerned that the school's email system is not used for bullying or harassing another student. Students found using the school's system or any non-school electronic device, including mobile phones, for cyberbullying should expect severe disciplinary action, up to and including expulsion.
- Students are expected to respect the privacy and ownership of others' work at all times. This includes not plagiarising information they find on the internet and presenting it as their own work, or copying work of other students, with or without permission, which is held in students' computer files.

Staff

All staff members should be aware of the following in relation to their use of school technology:

- **Copyright -** 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 License Agreement. Printing from CD-ROM or downloading and printing from the internet is allowed for the purpose of school related study and research. Software copying must be in accordance with legal requirements, and 'pirate' software is not permitted on any school owned computer.
- **Offensive material -** Deliberate attempts to seek, use or transmit material that is illegal or which would be regarded by reasonable persons as offensive is not permitted. Should offensive materials be received by staff members, they should be destroyed immediately. The school administration has the final say in deciding what is or is not offensive in the school context, but will be guided by Section 85ZE of 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.' **Use of the Internet in an offensive manner can result in criminal prosecution**.

- E**mployer Liability**- the school owns all messages and transmissions conducted through its system and therefore is legally responsible for all messages and transmissions. Staff should be aware that the school's computer system records all email and internet usage and, although *records of usage are not monitored on a systematic basis, nor are random checks undertaken on email and internet usage by staff, should an issue arise in relation to email and internet usage, the relevant records would be accessed.*
- **Technology Harassment**– the school complies with all anti-discrimination legislation. Staff should be aware that email harassment and/or technology harassment can occur on any of the grounds of discrimination. The school will not tolerate email and/or internet harassment. Any issue involving harassment or discrimination could result in disciplinary action.
- **Privacy** - Staff are required to maintain confidentiality with reference to student and family records and information, as outlined in privacy legislation. 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. Staff will be made aware through this policy and other appropriate forums e.g. staff meetings, of the need to maintain information security.
- **Access** - Computer systems at the School are protected by password access as well as physical barriers where possible. At no time should third parties be given unsupervised access to School records. Access to student, staff and family records will be given only on the authorisation of the Principal or his/her delegate where required by law or statutory authority. Staff should ensure that confidential documents or records are not left on desktops to be viewed by third parties, after hour's staff etc.
- **Viruses** – the school attempts to prevent and/or detect viruses by ensuring suitable virus detection software is maintained on computer networks within the School. External disks will not normally be accepted into School computer systems. If an external disk is used on a School computer, it must be scanned for viruses prior to being used. No shareware type external games disks should be used in a School computer. Files downloaded from the Internet are to be scanned for viruses. If files are in a zipped format, they are to be scanned prior to and after extracting the zipped file. Emails with attached files are also to be scanned for viruses. Please contact the IT Coordinator if you detect a virus on school equipment.
- **Security –** Staff should report any security breach, including suspected security weaknesses and software malfunctions, to the schools' system to the IT Coordinator immediately they become aware of the breach. Staff members should be aware that staff involvement in a security breach is considered serious and may result in an official warning, counselling or termination of a staff member's employment according to the severity of the breach.
- **Emails –** staff are asked to follow the procedures below when using the school's email system:
    - ***Use of disclaimer*** - All email messages should have the following Disclaimer included below your 'signature': *Disclaimer: Whilst every attempt has been made*

to ensure that material contained in this email is free from computer viruses or other defects, the attached files are provided, and may only be used, on the basis that the user assumes all responsibility for use of the material transmitted. This email is intended only for the use of the individual or entity names above and may contain information that is confidential and privileged. If you are not the intended recipient, please note that any dissemination, distribution or copying of this email is strictly prohibited. If you have received this email in error, please notify us immediately by return email or telephone (school number) and destroy the original message.

In the context of the School's Risk Management Strategy, *where appropriate*, email messages containing information or advice to parents/students/ school personnel and/or other organisations, should include the following Disclaimer (or similar): *The contents of this message are provided without responsibility in law for their accuracy or otherwise, and without assumption of a duty of care by the School.*

- ***Viruses - For incoming email*** – As *a matter of course all email attachments are checked automatically by virus protection software*. If there is any uncertainty about a file, the IT Coordinator should be consulted. 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 should probably be erased.

  For outgoing email – It is unlikely that any .COM or .EXE files will need to be sent. If they do, the files must be virus scanned before sending.
- ***Use for official purposes*** - Email is recognised as an official form of correspondence and therefore care should be taken to ensure that spelling, grammar and format are appropriate to the professional standards required for school communications. Where appropriate, copies of email messages should be printed and filed accordingly for future reference and access.
- ***Use for personal purposes*** - As applies to other communications, the use of email for personal purposes is permitted within reasonable limits. Email facilities cannot be used for any individual commercial activities.
- ***Absence from School*** - 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. Alternatively, for staff on a period of extended leave, arrangements can be made to have email forwarded to another address within the school. The appropriate arrangements should be made through the IT Coordinator.
- ***Action on emails***-All email messages should be actioned. Messages that are intended for another member of staff can be simply forwarded to that staff member.
- ***File Management*** - Email will work more efficiently if not clogged up with unwanted emails. If certain emails need to be kept, it is worthwhile creating new folder(s) to keep these safe. It is important to delete messages, when no longer required, from three areas – Inbox, Sent Files and Deleted Files. Good practice

would be to delete the files once a day if they are no longer required, and then delete the deleted files once a week.

- ***Copyright*** **-** As with all documents, staff should ensure that copyright provisions are followed in relation to materials transmitted by email.

POLICY RELEASE DETAILS

Date of Policy
January 2018

Approved by
Board

Review Date
Annually