Appendix 1

The Use of Personal Technology Devices* at School

This policy reflects the importance the school places on students displaying courtesy, consideration and respect for others whenever they are using personal technology devices.

**Personal Technology Devices**
The use of mobile phones, pagers, portable CD and MP3 players, Personal Digital Assistants and similar electronic devices in class is disruptive to the learning environment of all students and is banned from use during school hours.

**Personal Technology Device Etiquette**
Bringing personal technology devices to school is not encouraged by the school because of the potential for theft and general distraction and/or disruption associated with them. However, if they are brought to school, they must be turned off and out of sight during school hours or school functions (handed to school office – not in teachers’ desks/filing cabinets). Personal technology devices may NOT be used at morning tea and lunch breaks. Students wishing to use these devices in special circumstances must negotiate arrangements with the Principal.

**Confiscation**
Personal technology devices used contrary to this policy on school premises/school functions will be confiscated by school staff. They will be made available for collection from the school office at the end of the school day unless required to be kept for purposes of disciplinary investigation, when it will only be returned in the presence of a parent.

Devices potentially containing evidence of criminal offences may be reported to the police. In such cases police may take possession of such devices for investigation purposes and students and parents will be advised to contact Queensland Police Service (QPS) directly.

Students who have a personal technology device confiscated more than once will not be permitted to have a personal technology device at school for at least one month, or longer if deemed necessary by the Principal.

**Recording voice and Images**
Every member of the school community should feel confident about participating fully and frankly in all aspects of school life without concern that their personal privacy is being invaded by them being recorded without their knowledge or consent.

We uphold the value of trust and the right to privacy at Rasmussen State School. Students using personal technology devices to record inappropriate behaviours or incidents (such as vandalism, fighting, bullying, staged fighting or pranks etc) for the purpose of dissemination among the student body or outside the school, by any means (including distribution by phone or internet posting) builds a culture of distrust and disharmony.

Students must not record images anywhere that recording would not reasonably be considered appropriate (e.g. in change rooms, toilets or any other place where a reasonable person would expect to be afforded privacy). Recording of events in class is not permitted unless express consent is provided by the class teacher in relation to their curriculum program.

A student at school who uses a personal technology device to record private conversations, ordinary school activities or violent, illegal or embarrassing matter capable of bringing the school into public disrepute is considered to be in breach of this policy.
Even where consent is obtained for such recording, the school will not tolerate images or sound captured by personal technology devices on the school premises or elsewhere being disseminated to others, if it is done for the purpose of causing embarrassment to individuals or the school, for the purpose of bullying or harassment, including racial and sexual harassment, or where without such intent a reasonable person would conclude that such outcomes may have or will occur.

Students involved in:
- recording; and/or
- disseminating material (through text messaging, display, internet uploading etc); and/or,
- knowingly being a subject of a recording
- Breach of this policy may be subject to discipline (including suspension and recommendation for exclusion).

Students should note that the recording or dissemination of images that are considered indecent (such as nudity or sexual acts involving children), is against the law and if detected by the school will result in a referral to QPS.

Text communication
The sending of text messages that contain obscene language and/or threats of violence may amount to bullying and or harassment or even stalking, and will subject the sender to discipline and possible referral to QPS. Students receiving such text messages at school, should ensure they keep the message as evidence and bring the matter to the attention of the school office.

Assumption of cheating
Personal technology devices may not be taken into or used by students at exams or during class assessment unless expressly permitted by staff. Staff will assume students in possession of such devices during exams or assessments are cheating. Disciplinary action will be taken against any student who is caught using a personal technology device to cheat during exams or assessments.

Recording Private Conversations and the Invasion of Privacy Act 1971
It is important that all members of the school community understand that under the Invasion of Privacy Act 1971, ‘a person is guilty of an offence against this Act if the person uses a listening device to overhear, record, monitor or listen to a private conversation’. It is also an offence under the Act for a person who has overheard, recorded, monitored or listened to a conversation to which s/he is not a party to publish or communicate the substance or meaning of the conversation to others.

Students need to understand that some conversations are private and therefore to overhear, record, monitor or listen to such private conversations may be in breach of this Act, unless consent to the recording is appropriately obtained.

Special Circumstances Arrangement
Students who require the use of a personal technology device in circumstances that would contravene this policy (for example to assist with a medical condition or other disability or for a special project) should negotiate a special circumstances arrangement with the Principal.

* Personal Technology Devices includes, but is not limited to, games devices (such as Portable gaming devices, Tamagotchis®, laptop computers, PDAs, Blackberrys®, cameras and/or voice recording devices (whether or not integrated with a mobile phone or MP3 player), mobile telephones, iPods® and devices of a similar nature.

Education Queensland does not tolerate bullying behaviour at schools. This includes bullying conducted by electronic means.

** Please Note:
No liability will be accepted by the school in the event of the loss, theft or damage of privately own devices.
CONSEQUENCES FOR MISAPPROPRIATE USE OF PERSONAL TECHNOLOGY DEVICES

May include but not limited to:
- Warning
- Parent Involvement
- Confiscation of Device
- Withdrawal from class or playground
- Suspension
- Proposal or Recommendation for Exclusion

COMPUTER NETWORK BEHAVIOUR

Prohibited Activities

DOWNLOADING / STORAGE (Non-Study Materials):
- Software, Games, Music, Images and Files not relevant to study. (All Drives).
- Including (MP3, WMA, WAV, EXE, MID, MPEG, MOV, AVI, ASF, COM, ZIP) Files.

ACCESSING RESTRICTED AREAS OF CURRICULUM SERVER
- Copying, Deletion, or Moving of System Files on the Server.

REMOVAL / RELOCATION OF COMPUTER HARDWARE
- Swapping of Keyboards and Mice
- Removal / Replacement or Touching of Cable Connections.

STEALING OF COMPUTER HARDWARE
- Removal of Keyboards, Mouse, and Cables and parts from Machines.

ILLEGAL AND INAPPROPRIATE CONTENT VIEWING
- Accessing Pornography, Illegal Information, Racist, Sexist, and Offensive Materials.

INAPPROPRIATE USE OF EMAIL OR INTERNET
- Using emails/internet for non-educational purposes e.g. unfriendly statements towards other students/staff
- Using ‘social networking’ sites during school hours

CONSEQUENCES FOR INAPPROPRIATE COMPUTER NETWORK BEHAVIOUR

PRIOR WARNING
All students are reminded of the rules of using the computers especially in not giving out their passwords, or logging other people onto their computer. They are also reminded that if they suspect people know their password ask their teacher to get it changed.

FIRST OFFENCE: REMOVAL FROM NETWORK (1 WEEK). (Parents notified)
Access to Curriculum Network and Internet denied for 1 week, due to repeated breach of guidelines. Teachers informed to provide alternate work.

SECOND OFFENCE: REMOVAL FROM NETWORK (1 MONTH). (Parents notified)
Access to Curriculum Network and Internet denied for 1 month, due to constant breach of guidelines. Teachers informed to provide alternate work. Student will also be required to meet with Deputy Principal before reactivation of account.

THIRD OFFENCE: REMOVAL FROM NETWORK (INDEFINITE)
Access to Curriculum Network and Internet removed totally, due to blatant disregard of the guidelines. Teachers informed to provide alternate work. Administration will require a meeting attended by student and guardians to determine if and when student will be reallocated an account.
Appendix 2

**CYBERSAFETY INFORMATION**

**Cybersafety** is a broad term referring to appropriate and responsible behaviour online – it covers online privacy and information protection, good manners and behaviour online, and knowing how to get help to deal with online issues.

**Cyberbullying** is when technology, such as email, mobile phones, chat rooms and social networking sites, are used to verbally or socially bully another person. Bullying is an ongoing abuse of power to threaten or harm another person.

The following are some common examples of cybersafety issues, including cyberbullying:

- sending or posting abusive, threatening, humiliating or harassing messages via text, social networking sites or email
- forwarding others’ personal emails, messages, pictures or videos without their permission
- uploading embarrassing or degrading images or videos involving other children (including fight videos)
- taking and sending sexually explicit images of other children using mobile phone or web applications
- using social networking sites or blogs to post inappropriate photographs or messages about other children or school staff
- excluding children online through emails, chat and social networking sites
- imitating others or assuming a child’s identity, then sending and posting material which damages their social status or relationships with others
- making prank calls to another child’s mobile phone.

Parents can use a number of simple strategies to enhance cybersafety, such as:

- locate your computers in spaces which are visible and open, like a family room
- monitor or supervise your child on the internet and conduct some “shoulder surfing” or “spontaneous” observing when your child is online. Be aware of what your child is doing on the internet and display an interest in their cyberspace knowledge and experience
- discuss a plan with your child to address cybersafety and cyberbullying. Ensure they know you will be supportive if they report something to you
- reassure your child they will not lose access to their technology if they report anything to you. Many children see this as punishment
- review the age suitability of any social networking sites your child joins
- review your child’s ‘friends list’ on social networking sites to help you manage their safety and reduce the risk of them associating with inappropriate contacts
- educate yourself on the latest threats facing children online
- try to keep communication with your child open and positive so they trust you viewing their profile
- become a member of the social networking site and become an online friend of your child
- reinforce the need to keep passwords private and updated regularly, but consider having access to your child’s password yourself
- ensure your child understands the implications of posting images and other content on the internet

How can I promote my child’s cybersafety?

- educate your child about appropriate online behaviours.
  Take time to sit with your child and participate together on the internet. Assist in developing the knowledge they need to communicate responsibly and respectfully with friends, family and other internet users
- set clear rules about your child’s mobile phone and online activities. Talk with your child about which websites and internet activities they are allowed to access
- consider installing appropriate software which has the ability to limit internet usage times and monitor/restrict website activity
• Ensure you are aware of the software and app features installed on your child’s mobile phone, music or tablet device. Many apps have age suitability recommendations and require age confirmation prior to downloading/use.

Additionally, many devices support parental controls which prevent access to specific features or content. These controls can be enabled in the settings menu on your child’s device. Consult the device documentation for further information.

**EMAIL INTERNET AGREEMENT – sections signed by student and parent.**

While I have access to the Internet:
· I will use it only for educational purposes.
· I will use it only under teacher supervision;
· I will not look for anything that is illegal, dangerous or offensive;
· If I accidentally come across something that is illegal, dangerous or offensive, I will: Turn off the monitor and immediately and quietly inform my teacher. (This enables the site to be blocked)
· I will not download or print material without a teacher’s approval.
· I will respect copyright by not claiming the work of others as my own and I will acknowledge the information source.
· I will not reveal my home address or phone number or anyone else’s.
· I will not send a photo of myself or of anyone else via the Internet unless directed by a teacher as part of an e-mail exchange with another school.
· I will not use the Internet to annoy or offend anyone else.
· I will not reveal my personal or class access information to anyone else.
· I will not bring games or other programs into the school for use on school computers.
· I understand that the computer network may be set up differently to home computers and I understand that I should listen carefully to the instructions given by my teacher. I will not change any settings on the school computers.
· I will respect the equipment provided for my use by not vandalising, disrupting or harming the equipment.
· I will scan any disks for viruses on networked machines before using the disks on any school computers.
I understand that if the school decides I have broken these rules, appropriate action will be taken. This may include loss of my Internet access for some time and my parents being informed.