Reviewed December 2016
Governing Council Approved December 2016

LOCK AREA SCHOOL

ICT Acceptable Use & Cyber Safety Policy

Important terms used in this document:

a) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies.
b) **'Cyber Safety'** refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones
c) **'School ICT'** refers to the school's ICT equipment/device network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below
d) The term **'ICT equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, laptops, tablets, iPads, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), gaming consoles, robots, and any other, similar, technologies as they come into use.

Guidelines and Conditions for Appropriate Use of ICT Facilities

The Lock Area School network is provided for staff and students to promote educational excellence by facilitating resource sharing, innovation and communication. All students are given full access to the Lock Area School network with an individual account (R-10). Students also have school-administered individual electronic mail (Years 3-10) and full Internet access (R-10). Any such facilities must be regarded as privileges which may be withdrawn for misuse of the resources.

Computing facilities are provided primarily for the educational benefit of students and the professional development of staff. Any behaviour that interferes with these primary objectives will be considered an infringement of Acceptable Use.

1. General Policies

- Use of ICT equipment/Internet resources is for educational purposes.
- Appropriate language must be in all communications including email messages, chat and web pages.
- No user may deliberately or carelessly waste ICT resources (eg unnecessary printing) or disadvantage other users (eg by monopolising equipment, network traffic, etc).
- Consideration must be given to avoiding inconvenience to other ICT equipment users. Eg use headphones to listen to sound or music; leave ICT equipment/devices ready for the next user to log in; not leave programs running on ICT equipment/devices when you leave; not leave rubbish or paper lying around computers; replace furniture to normal positions when you leave.

2. Computer/Device Hardware

ICT facilities are expensive, sensitive and must be treated carefully.

Students must not:

- Connect any unauthorised device (eg a laptop/iPad from home) to the network at any time. Any such attempt will be regarded as a violation of network security.
- Do anything likely to cause damage to any equipment, whether deliberately or carelessly
- Steal equipment
- Vandalise equipment (eg graffiti)
- Mark or deface any equipment
- Interfere with networking equipment such as hubs
- Eat or drink near any School owned ICT equipment/devices
- Attempt to repair equipment
- Unplug cables or equipment
- Move equipment to another place
- Remove any covers or panels
- Disassemble any equipment
- Disable the operation of any equipment
- Tamper with ICT equipment/devices in any way, without explicit instructions from staff

- Use devices to find, create or send information that might be harmful, inappropriate or hurtful to themselves or anyone else

Students must also report other people breaking these rules.

3. Software and Operating Systems

Computer/device operating systems and other software must be set up properly for ICT equipment/devices to be useful.

Students will not:

- Change any ICT equipment/device settings (including screen savers, wallpapers, desktops, menus, standard document settings, etc) without permission.
- Add personalised pass locks on ICT equipment/devices
- Bring or download unauthorised programs, including games, to the School or run them on school ICT equipment/devices. Online Internet games are banned during lesson time.
- Delete, add or alter any configuration files.
- Copy any copyrighted software to or from any ICT equipment/device, or duplicate such software.
- Deliberately introduce any virus or program that reduces system security or effectiveness.

4. Networks

Network accounts are to be used only by the authorised owner of the account. If you find a computer logged in, you should do nothing in that account except log out.

It is the responsibility of students to make backup copies of their work. The School will exercise due care with backups but will not be held responsible for lost data.

Students must not:

- Use or download peer to peer file sharing programs such as but not limited to Limewire or U-torrent which are expressly forbidden.
- Possess evidence of previous use in their network directory.
- Attempt to log into the network with any user name or password that is not their own, or change any other person's password.
- Reveal their password to anyone except the system administrator or classroom teachers, if necessary. Students are responsible for everything done using their accounts, and everything in their S Drive, on their allocated iPad or any other personal device. Since passwords must be kept secret, no user may claim that another person entered their home directory and did anything to cause school rules to be broken.
- Use or possess any program designed to reduce network security.
- Enter any other person's allocated iPad or home directory (drive S:) or do anything whatsoever to any other person's files.
- Attempt to alter any person's access rights.
- Store the following types of files in their home directory, without permission from the Computer Systems Manager:
    - Program files (EXE, COM)
    - Picture files, unless they are required by a subject
    - Obscene material – pictures or text
    - Obscene filenames
    - Inappropriate material
    - Insulting material
    - Password-protected files
    - Copyrighted material
- Intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

5. Printing

Students must minimise printing at all times by print previewing, editing on screen rather than on printouts and spell-check before printing. Abuse of printing privileges may result in individuals being invoiced for printing.

Students must not load paper into printers without supervision. Paper that is pre-used, torn, creased, damp, irregularly shaped or sized or unsuitable for laser printers should not be used in laser printers.

Where possible, Internet information is to be transferred to a Word document before attempting to print. Use of the colour printers is to be only used for final copies (unless otherwise negotiated with relevant staff) and completed with teacher consent. Cost for this printing is greater than other laser printers and are to be determined by the network administrator.

6. Internet usage

Internet access is expensive and has been provided to assist students' education. Students must use it only with permission, and not in any unauthorised way. It is not intended for entertainment. Abuse of Internet privileges may result in individuals being invoiced for excess usage.

Because the Internet is an unsupervised environment, the school has a responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, filtering software has been placed on the Internet links. In the end, however, it is the responsibility of individual students to ensure their behaviour does not contravene school rules or rules imposed by parents/guardians. The school is aware that definitions of "offensive" and "inappropriate" will vary considerably between cultures and individuals. The school is also aware that no security system is perfect and that there is always the possibility of inappropriate material, intentionally and unintentionally, being obtained and displayed.
It is the responsibility of the school to:-

- provide training on the use of the Internet and make that training available to everyone
- take action to block the further display of offensive or inappropriate material that has appeared on the Internet links

6.1 Email, Instant Messaging & Air Dropping

Electronic mail is a valuable tool for personal and official communication both within the School network and on the Internet. Students and staff are encouraged to use it and take advantage of its special features. As with all privileges, its use involves responsibilities.

Since students are given free email accounts by the School, no other email accounts may be used at the School. If they have other email accounts, they must check for mail and collect it at home. Other email accounts such as **Hotmail** must **not** be used on School computers, unless a need for brief access is required for school purposes.

Throughout the Internet there are accepted practices known as Netiquette which should be followed. The following points should be noted:

- Use appropriate language and be polite in your messages. Do not be insulting, abusive, swear or use vulgarities.
- Never write hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviours. Therefore no messages should contain obscene comments, threats, sexually explicit material or expressions of bigotry or hate.
- Do not reveal personal addresses or the phone numbers of students or colleagues.

Please note that email is not guaranteed to be private. System administrators do have access to all files including mail. Messages relating to illegal activities may be reported to the authorities.

Students will not:

- Use air dropping or real-time social networking programs (such as but not limited to MIRC, ICQ, Yahoo Messenger, MSN Messenger, Facebook, Twitter, Instagram, etc) unless instructed by a teacher
- send offensive mail/messages
- send unsolicited mail/messages to multiple recipients ("spam")
- use email/messaging for any illegal, immoral or unethical purpose
- attempt to disguise their identity or the true origin of their mail/messaging
- forge header messages or attempt to use any mail server for deceptive purposes
- use any mail program designed to send anonymous mail

6.2 World Wide Web

The World Wide Web is a vast source of material of all sorts of quality and content. The School will exercise care in protecting students from offensive material, but the final responsibility must lie with students in not actively seeking out such material. It is conceivable that, especially for senior students, information is required for curriculum purposes that may appear to contravene the following conditions. In such cases, it is the responsibility of students and teachers to negotiate the need to access such sites.

Students will not deliberately enter or remain in any site that has any of the following content, unless specifically instructed by a teacher to do so in the context of the curriculum being taught:

- Nudity, obscene language or sexual discussion intended to provoke a sexual response
- Violence
- Information on, or encouragement to commit any crime
- Racism
- Information on making or using weapons, booby-traps, dangerous practical jokes or "revenge" methods

If students encounter any such site, they must immediately turn off the computer monitor (not the computer itself) and notify a teacher. Do not show your friends the site first.

- Students will not attempt to circumvent the schools content filtering system by using proxy by-pass sites or any other means. Students viewing blocked sites will be deemed to have deliberately interfered with network security and corresponding sanctions will apply.
- The Internet must not be used for commercial purposes or for profit.
- The Internet must not be used for illegal purposes such as spreading viruses or distributing/receiving software that is not in the public domain.
- It is inappropriate to act as though you intend to break the law e.g. by attempting to guess a password or trying to gain unauthorised access to remote devices. Even if such attempts are not seriously intended to succeed, they will be considered serious offences.
- Interactive use of the Internet should ensure that there is no possibility of the transmission of viruses or programs which are harmful to another user's data or equipment.
- Copyright is a complex issue that is not fully resolved as far as the Internet is concerned. It is customary to acknowledge sources of any material quoted directly and it is a breach of copyright to transmit another user's document without their prior knowledge and permission. This includes the use of images and text. It is safest to assume *all* content on web sites is the legal property of the creator of the page unless otherwise noted by the creator.

Monitoring

The School is required to exercise its right to monitor the use of the School's ICT resources to:

- Ensure that the systems and networks are functioning properly
- Protect against unauthorised access
- Ensure compliance with the ICT Acceptable Use Policy

Personal Electronic Devices (student owned devices including mobile phone, iPod or other ICT mobile device)

Important information for this section of the document:

a) Personal Electronic Devices in this document refers to mobile phones, iPods, iPads, MP3 Players, Cameras or any other electronic device brought from home and does not belong to the school.

b) This section of the Acceptable Use and Cyber Safety Policy also applies to students during school excursions, camps and extra-curricular activities.

c) In some instances, off site and after hour’s cyber bullying may be punishable by law.

The school acknowledges that some students may need to carry personal electronic devices to and from school, however if students bring them to school, they do so at their own risk. Lock Area School cannot accept responsibility for any personal electronic devices that goes missing nor does it have the resources to conduct investigations into misplaced or stolen devices.

If changes are made to a student's routine that affect the school, it is essential that the school is contacted via the front office so that it can carry out its Duty of Care. We believe that it is critical that all students are given the best learning environment in which to learn without interruptions created by personal electronic device use in lesson time.

In order to maximise the learning opportunities for every student the following guidelines are to be followed:

- All personal electronic devices must be switched off and in bags at all times during the school day/event.
- The sending and receiving of text messages must not occur during lesson time or during any school activity/event.
- Communication between staff and students should only be used in exceptional and agreed circumstances, otherwise the school phone should be used
- Not use personal electronic devices to take images of students or staff without the agreement of the other party. No photographs or videos taken in school should be uploaded to the Internet unless specific permission has been granted.
- Report incidents of bullying using personal electronic devices to teachers in the first instance. Bullying by text will be treated in the same severe manner as any other form of bullying.
- Not use music / video players (eg iPods) during lessons unless the teacher has given permission, or a medical condition exists that requires the use of such.
- Will not break copyright laws by swapping illegal music/video files.

If students are using a personal electronic device during the school day/event they can expect to have the device removed from them and taken to the front office for the remainder of the school day/event. If there are any issues concerning a student's use of a personal electronic device during class time, then parents will be contacted.

All children have the right to feel safe and supported in their learning and playing times at Lock Area School. Inappropriate use of personal electronic devices will result in consequences being applied and if necessary SAPOL will be contacted.

The school will apply the guidelines of the Behaviour Management Policy to offending students. In extreme circumstances an offending student could be excluded from school.

Management of Infringements

Breaches of the conditions of this ICT Acceptable Use and Cyber Safety Policy may result in access restrictions or termination to ICT resources, apart from other sanctions deemed appropriate by the School, including suspension and expulsion.

Lock Area School, nor its staff, will be liable or held responsible for damage or loss of equipment under any circumstances.

Personal ICT equipment is the responsibility of the individual at all times, and is only to be used in accordance with the school ICT Acceptable Use and Cyber Safety Policy, with particular regard to Network Internet Access which is regulated and filtered. – ie Internet dongles are not permitted.

School equipment and facilities are to be restricted to suitable school use at all times, and are to be used in accordance with the school ICT Acceptable Use and Cyber Safety Policy.

The following is a list of possible penalties:

- temporary ban on using ICT equipment/devices
- removal of email/air dropping privileges
- removal of Internet-access privileges
- removal of network access
- removal from classes where ICT equipment/devices are involved
- loss of marks for an assessment task (where appropriate)
- suspension from school
- repair/replacement ensuring any material damage caused to the School's ICT resources (infrastructure, hardware or software) will be billed to the parent/guardian

If you break the law you may be liable for prosecution.

Action Principals can take for Incidents of Cyber Bullying or Electronic Crime

Bullying has taken on a new dimension with the introduction of new forms of electronic communication. Cyber bullying can be perpetrated at any time of the day or week. This behavior can threaten the safety or wellbeing of others.

Under regulations 40 and 41 of the Education Regulations 1997, principals can suspend or exclude a student who acts in a manner that threatens the safety or wellbeing of a student or member of staff, or another person associated with the school. These regulations do not preclude an event that occurs outside of school hours or off-site. Principals can therefore use these procedures with a student enrolled at their school if the principal believes, on reasonable grounds, that the student has acted in such a manner, **even if this behavior occurred outside of school hours or off site**.

Police officers also have the power to confiscate a mobile phone where any image held on the phone is possible evidence of a crime. The phone may be kept by SAPOL until the action comes before a court. Where DECD staff reasonably suspect that a student has used a mobile phone to record a crime, the phone should be confiscated and handed to SAPOL.

LOCK AREA SCHOOL
ICT ACCEPTABLE USE POLICY

STUDENT ACCOUNTABILITY AGREEMENT

PLEASE RETURN THIS PAGE ONLY TO SCHOOL

STUDENT SECTION – to be completed by the student

Student Name (please print): .... Year Level: ....

Student Declaration

- I have read the Lock Area School ICT Acceptable Use and Cyber-Safety Policy, which sets out the policy, guidelines and conditions to be met when using ICT hardware, software and operating systems, school networks, the Internet and personal electronic devices.
- I understand the content of the document and I agree to adhere to the policy, guidelines and conditions as set out in the document.
- If I disagree with any aspects of the policy and do not wish to abide by the terms within, I will notify any member of the ICT staff immediately and cease using the facilities.
- I understand and accept that monitoring processes are in place to protect Lock Area School students, and that school workstations can be remotely viewed and controlled by system administrators.
- I understand and accept that backing up of my files on a regular basis is my responsibility, and that the School is not liable for any loss of work due to computer failure.
- I will not hold any staff member at Lock Area School responsible for, or legally liable for, materials distributed to, or acquired from, the network or broader Internet.
- Any materials that I produce, including email/messages, will portray me as a positive ambassador for my school.

Student Signature: .... **Date:** ....

PARENT/CAREGIVER Consent

Parent Name (please print): .... Phone: ....

Parent/Guardian Declaration

- I have read the Lock Area School ICT Acceptable Use and Cyber-Safety Policy, which sets out the policy, guidelines and conditions to be met when using ICT hardware, software and operating systems, school networks, the Internet and personal electronic devices.
- I have discussed the content of the document with my child and I agree that they should adhere to the policy, guidelines and conditions as set out in the document.
- I will not hold any staff member at Lock Area School responsible for, or legally liable for, materials distributed to, or acquired from, the network or broader Internet.
- I understand the consequences if my child does not abide by the content of the document and accept that such action may result in loss of the privilege to use the school computer network system apart from other sanctions deemed appropriate by the school.

Parent Signature: .... **Date:** ....