Roxburgh Homestead Primary School
ESMART GUIDELINES, POLICY & AGREEMENT

Introduction:
Roxburgh Homestead Primary School aims to provide an educative environment by establishing an eSmart culture which is in keeping with the values of the school, legislative and professional obligations, and the community's expectation. Within this context, the objective of the eSmart Guidelines is to ensure the smart, safe, responsible use of ICT within the school community.

The eSmart Guidelines outlines the conditions applying to the use of all ICT devices, technologies and online environments and behaviours associated with safe, responsible and ethical use of technology at Roxburgh Homestead Primary School. Authorised users are required to comply with the Guidelines.

Roxburgh Homestead Primary School strongly believes that children and young people have the right to participate in an education system which values and promotes safe, respectful and ethical attitudes and behaviours and prepares them for successful relationships and interactions in their adult lives. Creating and maintaining respectful, safe, secure and stimulating learning environments is an essential characteristic of a school that is engaging and inclusive of a diverse range of learners.

A school also has a Duty of Care responsibility to identify known and foreseeable risks to students and to take reasonable steps to minimise these risks and to support students in their care. This includes online and digital environments, ICT devices and technologies, particularly those that are created and/or owned by the school and its teaching staff.

Roxburgh Homestead Primary School believes the teaching of cybersafe and responsible online behaviour is essential in the lives of students and is best taught in partnership between home and school. Students of the 21st century spend increasing amounts of time online, learning and collaborating. To be safe online and to gain the greatest benefit from the opportunities provided through an online environment, students need to do the right thing by themselves and others online, particularly when no one is watching.

Safe, responsible and ethical behaviour is explicitly taught at our school and parents/carers are requested to reinforce this behaviour at home.

Some online activities are illegal and as such will be reported to police.

Definitions of terms used in the eSmart Guideline.

a. '**Authorised user'** means a person who has signed the eSmart Agreement (or has had it signed on their behalf by a parent) and is authorised by Roxburgh Homestead Primary School to use school ICT.
b. **Cyberbullying** involves the use of information and communication technologies, such as email, mobile phone and pager text messages, instant messaging (IM) and defamatory personal websites, to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others
c. **'eSmart'** refers to the safe, responsible and ethical use of ICT. Other terms that have the same meaning include **'Cybersafety'** and **'Cybersmart'**.
d. **'Information & Communication Technology (ICT)'** is the term used to describe all the hardware (computers, mobile phones, cables, network facilities) and software (websites, computer programs) that allows data to be digitally processed, stored and communicated. ICT can be used to access, process, manage and present information; model and control events; construct new understanding; and communicate with others.
e. **'Network facilities'** includes, but is not limited to, intranet and internet access to files, web sites and digital resources via the school wireless network.
f. **'Digital Footprint'** is used to describe the 'trail' or 'presence' that is left on the internet. Anything that is posted to the Internet can remain online forever, even after it has been 'deleted'.
g. **'Communication technologies'** includes, but is not limited to, communication made using ICT equipment/devices such as the Ultranet, internet, intranet, email, instant messaging, social networking sites (including but not limited to Facebook, Twitter, Pinterest and so on), online discussions/surveys and mobile devices such as phone and tablet activities and related applications.

h. **'Social networking sites'** describes any website that allows users to create a public profile within that website and form relationships with other users who access the users profile. This includes but is not limited to community-based websites, online discussion forums, wikis, blogs, chatrooms and social spaces online such as Facebook, Twitter, Pinterest, YouTube. Other terms with the same meaning include **'social media', 'Web 2.0'** and **'online media'**.
i. **'eLearning tools'** includes, but is not limited to, the Ultranet and any online applications and programs that are used for educational purposes.
j. **'ICT equipment/devices'** includes, but are not limited to, computers (such as desktops, laptops, tablets), storage devices (such as USB and flash memory devices, CDs, DVDs, MP3 players), cameras (such as video, digital, webcams), all types of mobile devices including phones and tablets, and any other, similar, technologies as they come into use. This also refers to any device which connects to the school's wireless network.
k. **'Ultranet'** is a state-wide secure site that students, parents and teachers can access via the Internet. Students will participate in online learning activities that encourage them to create, collaborate and communicate their learning. Parents will have online access to keep up-to-date with their child's progress at school with learning activities, assessment and attendance.
l. '**Agreement'** refers to this eSmart Guildeline and any related ICT, Student Engagement and Wellbeing policy and agreement which may be developed by the school from time to time.
m. **'School'** refers to Roxburgh Homestead Primary School, the students, staff and parents.
n. **'School related activity'** includes, but is not limited to, an excursion, camp, sporting or cultural event, wherever its location.
o. **'School ICT'** includes, but is not limited to, network facilities, communication technologies, eLearning tools and ICT equipment/devices.
p. **'Objectionable material'** deals with matters such as pornography, cruelty, violence, or material of a discriminatory nature that it is likely to be injurious to the good of students or incompatible with the school environment. Other terms that have the same meaning include **'Inappropriate material'** and **'Unacceptable material'**.
q. **'Unacceptable student conduct'** includes, but is not limited to, malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, non-sanctioned gaming, impersonation/identity theft, copyright infringement, or cheating in an examination.
r. **'Educational purposes'** means activities that are directly linked to curriculum related learning.

Policies & Agreements in Place

- eSmart Guidelines – whole school
- eSmart Acceptable Use Agreement (Junior & Senior School) – student use
- Acceptable Use Policy for DEECD ICT Systems – for all STAFF
- Safe School Policy (Cybersafety, Anti-bullying, Social Media, Student Wellbeing) – whole school
- Electronic Devices, Photo, Video & Online Media Policy – whole school and student use

Breach of eSmart Guidelines

Breaches of the eSmart Guidelines, associated Policies & Agreements, can undermine the values of the school and the safety of the eLearning environment, especially when ICT is used to facilitate misconduct. Such a breach which is deemed by the school to be harmful to the safety of the school may possibly result in serious disciplinary action such as:

1. Withdrawal of access to the school network and devices
2. Confiscation of personal devices used inappropriately throughout the school day, including, but not limited to, school cultural or sport events, and during camps/excursions
3. Suspension or withdrawal of enrolment in cases of serious misconduct
4. It is a criminal offence to use an ICT device to menace, harass, make threats, or offend another person. In these instances, the school may consider it appropriate to involve police.

In investigating a suspected breach of this eSmart Guildelines, and associated Policies and Agreements, the Authorised User agrees to promptly make the ICT equipment/device available to the school for the purpose of any investigation and/or audit and to cooperate otherwise with the school in any investigation or audit process.

The terms of this eSmart Guildeline form part of the School's expectations for the purposes of a student's enrolment at the school and the conditions of enrolment.

User eSmart Obligations

1. Authorised Usage and eSmart Agreement

1.1. As the School provides network access, the contents of the School ICT system, including the Ultranet and email messages, remain the property of DEECD and the school. The school has the

capacity to monitor and control the system and reserves the right to monitor individual usage and report, where necessary, any indications of misconduct or prohibited use.
1.2. All users, whether or not they make use of network facilities and communication technologies on school owned or personal ICT equipment/devices, will be issued with the eSmart Acceptable Use Agreement. This document should be read carefully with the acknowledgement page signed and returned to school to gain access to the network facilities and ICT equipment/devices.
1.3. The school's ICT, including network facilities, communication technologies, eLearning tools and ICT equipment/devices cannot be used until the acknowledgement page of this Agreement has been signed and returned to your child's classroom teacher. Signed Agreements will be filed in a secure place.
1.4. It is recommended that authorised users keep the the eSmart Guideline, Policy and Agreement for reference. If necessary, a replacement copy will be supplied by the classroom teacher upon request.
1.5. The School encourages anyone with a query about the eSmart Guideline, Policy and Agreement to contact your child's class teacher (primary in the first instance.

2. Obligations and requirements regarding appropriate use of ICT in the School learning environment

2.1. While at School, using School owned or personal ICT equipment/devices, including mobile phones, is for educational purposes only.
2.2. When using School or privately owned ICT on the School site or at any School related activity prohibited use includes, but is not limited to, any conduct that is defined as objectionable and inappropriate:

- Would cause offense to students, teachers or parents, such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism, sexism, is derogatory or threatening to another e.g. libellous, slanderous, inflammatory, threatening, harassing;
- Has intention to deceive, impersonate or misrepresent;
- Forwards confidential messages to persons to whom transmission was never authorised by the School, including persons within the School community and persons/organisations outside the School community;
- Fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus;
- Breaches copyright;
- Attempts to breach security and infrastructure that is in place to protect user safety and privacy;
- Uses DEECD and staff emails for a purpose other than educational communication;
- Propagates chain emails or uses groups and lists inappropriately to disseminate information;
- Inhibits the user's ability to perform their duties productively and without unnecessary interruption;
- Interferes with the ability of others to conduct the business of the school;
- Involves malicious activity resulting in deliberate damage to School ICT and/or ICT equipment/devices;
- Involves the unauthorised installation and/or downloading of non-DEECD endorsed software;
- Breaches the ethos and values of the School.

2.3. In the event of accidental access of such material, Authorised Users must:

- Not show others;
- Shut down, close or minimise the window;
- Report the incident immediately to the classroom teacher, ICT coordinator, ICT technician, supervising teacher or Principal.

2.4. A person who encourages, participates or otherwise knowingly acquiesces in prohibited use of School, or privately owned communication technologies, on the School site or at any School related activity, may also be found to have engaged in prohibited use (Refer to eSmart Acceptable Use Agreement).

2.5. While at the School or a School related activity, Authorised Users must not have involvement with any material which might place them at risk. This includes images or material stored on privately owned ICT equipment/devices brought onto the School site, or to any School related activity such as USB or portable storage devices.

2.6. Authorised users must not attempt to download, install or connect any unauthorised software or hardware onto School ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies that are

available. Any Authorised Users with a query or a concern about that issue must speak with the relevant class teacher or ICT Coordinator.

3. Monitoring by the College

The School:

3.1. Reserves the right at any time to check work or data on the School's computer network, email, internet, Ultranet, computers and other School ICT equipment/devices, without obtaining prior consent from the relevant Authorised User.

3.2. Reserves the right at any time to check work or data on privately owned ICT equipment on the School site or at any School related activity. The Authorised User agrees to promptly make the ICT equipment/device available to the School for purposes of any such check and to otherwise co-operate with the School in the process. Before commencing the check, the School will inform the Authorised User, and their parent/guardian/carer of the purpose of the check.

3.3. Has the capability to restrict access to certain sites and data, record email and internet use, including the user details, time, date, sites visited, length of time viewed, and from which computer or device.

3.4. Monitors traffic and material sent and received using the School's ICT infrastructures. From time to time this may be analysed and monitored to help maintain an eSmart learning environment.

3.5. From time to time conduct an internal audit of its computer network, internet access facilities, computers and other School ICT equipment/devices, or may commission an independent audit of content and usage.

4. Copyright, Licensing, and Publication

4.1. Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Authorised Users must not breach laws of copyright, moral right or intellectual property – this includes, but is not limited to, illegal copies of software, music, videos and images.

4.2. All material submitted for internal publication and on the Ultranet must be appropriate to the School environment and copyright laws.

5. Individual password logons to user accounts

5.1. If access is required to the School computer network, computers, Ultranet and internet access using School facilities or privately owned devices, it is necessary to obtain a personal user account from the School.

5.2. Authorised Users must keep usernames and passwords confidential and not share them with anyone else. A breach of this rule could lead to users being denied access to the system, network facilities and ICT equipment/devices.

5.3. Authorised Users must not allow another person access to any ICT equipment/device logged in under their own user account. Material accessed on a user account is the responsibility of that user. Any inappropriate or illegal use of the computer facilities and other college ICT equipment/devices can be traced by means of this login information.

5.4. Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the eSmart Guideline, Policy and Agreement. This includes ensuring that no electronic communications could cause offence to others or harass or harm them, put the owner of the user account at potential risk, contain objectionable material or in any other way be inappropriate in the School environment.

5.5. For personal safety and having regard to Privacy laws, Authorised Users must not reveal personal information about themselves or others. Personal information may include, but is not limited to, home or email addresses, and any telephone numbers, including mobile numbers.

6. **Other Authorised User obligations**

6.1. Avoid deliberate wastage of ICT related resources through actions such as unnecessary printing and unnecessary internet access, uploads or downloads.

6.2. Avoid involvement in any incident in which ICT is used to send or display electronic communication, graphics, audio, video files which might cause offence to others and/or involve objectionable material.

6.3. Abide by copyright laws and obtain permission from any individual before photographing, videoing, recording, posting or publishing them.

7. Privacy

7.1. School ICT and electronic communication should never be used to disclose personal information of another except in accordance with the School's privacy agreement or with proper authorisation. The Privacy Act requires the School to take reasonable steps to protect the personal information that is held by the School from misuse and unauthorised access. Authorised Users must take responsibility for the security of their computer and not allow it to be used by unauthorised persons.

7.2. While **after school use** of communication technologies by students is the responsibility of parents, School policy requires that no student attending the School may identify, discuss, photograph or otherwise publish personal information or personal opinions about School staff, fellow students or the School. Any such behaviour that impacts negatively on the high public standing of the School may result in disciplinary action. The School takes a strong position to protect privacy and prevent personal information and opinion being published over technology networks including Facebook, You Tube, Tumblr, Twitter (and any further new technology).

8. Procedures for Mobile Phone and Mobile Device Use at School

Roxburgh Homestead Primary School accepts that parents provide their children with mobile phones to protect them from everyday risks involving personal security and safety. There is also ever-increasing concern about children travelling alone on public transport or commuting long distances to school. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can speak with their child quickly, at any time.
However, while at School, using School owned or personal ICT equipment/devices, including mobile phones, is for educational purposes in the first instance to ensure the benefits that mobile phones provide (such as increased safety and security) can continue to be enjoyed by our students.

Responsibility

8.1. It is the responsibility of students who bring mobile phones onto School premises to adhere to the guidelines outlined in this document.

8.2. The decision to provide a mobile phone to their children should be made by parents or guardians.

8.3. Parents should be aware and discuss the responsibility if their child takes a mobile phone onto School premises.

8.4. All mobile phones are to be handed into the classroom teacher at the beginning of the day.

8.5. Mobile phones will be kept securely by the classroom teacher during the day.

8.6. Students are required to mark their mobile phone clearly with their name.

8.7. Mobile phones which are found in the School and whose owner cannot be located are to be handed in to the School office.

8.8. The School accepts no responsibility for replacing lost, stolen or damaged mobile phones. Their safety and security is wholly in the hands of the student.

8.9. The School accepts no responsibility for students who lose or have their mobile phones stolen while travelling to and from school.

8.10. It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phone and/or passwords may not be shared.

8.11. Students protect the privacy and dignity of individuals and security of information, to maintain the high public standing of the School and compliance with State and Federal laws.

8.12. Mobile phones are switched off during classroom lessons unless under the instruction of the teacher when being used for educational purposes. Exceptions may be permitted in rare circumstances, should the parent/guardian specifically request it. Such requests will be handled on a case-by-case basis, and should be directed to the Principal.

8.13. If students need to check messages or voicemail they are permitted to do so during recess and lunch breaks.

8.14. The use of headphones is not permitted at School unless under the instruction of a teacher when being used for educational purposes. The School strongly advises that for safety reasons headphones are not used when students are traveling to and from school, eg. walking, riding a bike, moving on and off buses.

8.15. In accordance with School policies, any mobile phone being used inappropriately during the school day will be confiscated.

Parents are reminded that in cases of emergency, the School's Administration Office remains a vital and appropriate point of contact and can ensure your child is reached quickly, and assisted in the appropriate way. Phone calls home to parents are to be made by a staff member. Parent's can assist by reinforcing the eSmart Guidelines, Policy and Agreement with your child.

References /Resources/Agreements and Policies:

- Spring Gully Primary School - http://www.sgps.vic.edu.au/File.axd?id=b3b81425-1778-47f2-a3d0-ad4807cb178b
- Trinity Lutheran College - http://www.tlc.qld.edu.au/files/pdf/Policies%20and%20Procedures/eSmart-Policy-and-Agreement-Primary.pdf
- eSmart - https://www.esmartschools.org.au/eSmartsystemtool/system%20pages/tools.aspx
- Learning Online, DEECD - http://www.education.vic.gov.au/management/lol/default.htm
- ACMA - http://www.cybersmart.gov.au/Glossary.aspx

Cybersmart program –Australian Communication and Media Authority www.acma.gov.au
Cybersafety Outreach Program - Australian Communication and Media Authority www.acma.gov.au
www.cybersmartkids.com.au
www.commonsense.org

This policy will be reviewed as part of the schools three year review cycle.

This policy was ratified by school council in August 2014.

Parent Help – Roxburgh Homestead Primary School eSmart Guidelines, Policy & Agreement Guide
The following is a guide to the rules covered by the Agreement and to help you discuss these rules with your child.

1. **In agreeing to the terms of enrolment at Roxburgh Homestead Primary School I am accepting the college's eSmart Agreement.** eSmart policies are becoming accepted as an essential part of cybersafety and student wellbeing measures and programs for schools and other organisations including business.

2. **I can use personal and School ICT devices at school for educational purposes only.** This helps to ensure the equipment is available when students need to use it for their learning. It will also help to reduce the likelihood of any inappropriate activities taking place which put at risk the safety of the eLearning environment.

3. **If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.** This helps students to take responsibility for their own actions and seek advice when they are unsure of what to do. It provides an opportunity for the teacher and student to work through an issue and so avoid the student making an unwise decision which could possibly lead to serious consequences. All students require ongoing advice and guidance to help them become safe and responsible users of ICT.

4. **I will follow the eSmart rules, and will not join in if others are being irresponsible. If I become aware of others being irresponsible I will tell the teacher straight away.** Unfortunately, along with many benefits, technology has also provided new ways of carrying out anti-social activities. Often students become involved in these acts through peer pressure, without thinking of the consequences.

5. **If I accidentally come across inappropriate material I will tell the teacher straight away, without showing any other students.** Because anyone at all can publish material on the Internet, it does contain material which is inappropriate, and in some cases illegal. The School has taken a number of steps to prevent this material from being accessed. However, there always remains the possibility that a student may inadvertently stumble across something inappropriate. Encouraging students to tell a teacher immediately if they think something is inappropriate encourages students to take responsibility for their actions and keep themselves and others safe.

6. **I will log on with only my own username and password. I will not share my log on details with any other person. I will log off computers or shut down computers when I have finished using them or before letting someone else use the computer.** Passwords perform two main functions. Firstly, they help to ensure only approved persons can access the School ICT facilities thereby protecting personal work, files and emails. Secondly, they are used to track how those facilities are used. Knowing how the equipment is being used and by whom, helps the School to maintain an eSmart environment for all users, and teaches students the life skill of the importance of personal safety. Logging off, stops others from using a computer under your student's username. When the computer is started up again, the next user has to enter their own details to log on.

7. **I will not bring software or games from outside the college to use on the college network.** Schools must abide by any licensing requirements included within the software. This means unless the School or DEECD has purchased a copy, it will not usually be legally entitled to install the software.

8. **I will check with the teacher before using School equipment to copy software, music, videos or other files in case they breach copyright laws.** Any such copying is likely to be restricted by copyright laws. The School does not condone the use of its equipment for these activities.

9. **I will not use School ICT equipment, devices or network to be mean, rude, offensive, or to harass any member of the college community while at school or any school related activity. The same rule applies when using ICT at any time, WHETHER AT SCHOOL OR NOT.** The basic principles of courtesy and mutual respect extend to the use of information and communication technologies. The capacity of ICT to increase the scale and scope of misconduct can make an otherwise minor rule infringement into a much more serious matter. This includes the creation of abusive websites or the publishing of unacceptable material on social networking site.

10. **I will not share personal information about myself or others when using School ICT – this includes home and email addresses and phone numbers.** This reduces the risk of your child, or other students, being contacted by someone who wishes to upset or harm them, or use their identity for purposes which might compromise the student's privacy or security online.

11. **If I am not feeling safe at any time while using the college's ICT equipment, I will tell the teacher immediately.** The college strives to create a safe and secure eLearning environment for all students. Examples of situations involving the use of ICT which might cause a student to feel unsafe could include: contact being made by a stranger through email or text message, the presence of offensive images on a computer screen, an/or misconduct by other students. School staff need to be made aware of such situations as soon as they occur to ensure the college can respond immediately.

12. **If I do not comply with the School expectations, the School may need to talk to my family about what has happened. In very serious cases, the School may take disciplinary action including suspending me or withdrawing my enrolment from the School.** Depending on the seriousness of a particular breach, possible School responses could include one or more of the following: a discussion with the student, informing parents, loss of ICT privileges, the family possibly having responsibility for the cost of ICT repairs or replacement, the School taking disciplinary action such as suspension or withdrawal of enrolment, or in extreme circumstances reporting the offence to the police.

13. **I must abide by the rules of the School in relation to communication technologies while on School premises, or School related activities.** The devices referred to in this rule include those specified in the Agreement such as MP3 players, mobile phones, iPads, laptops and desktop computers. It is important to discuss the School's stance regarding the confiscation of mobile phones and mobile devices if used socially, inappropriately or turned on during lessons. This is an opportunity to have a discussion with your child about the appropriate use of ICT whether in or out of school. It helps keep students eSafe if they understand that many of these rules should be followed regardless of whose ICT equipment they are using, where they are, or who they are with.

www.education.vic.gov.au - Learning on Line/ Working on the Web
www.thinkuknow.org.au
www.staysmartonline.gov.au -Budd-e program
SGPS ICT Scope and Sequence program chart
eSmart Schools Program
Netbook Agreement / SGPS ICT Behaviour Management Plan /Acceptable Use Policy for DEECD ICT Systems
SGPS Cybersafety Policy / SGPS Electronic Devices Policy/ SGPS eSmart Guidelines
Date: September 2010