St Pauls Catholic College
Student Acceptable Use of ICT Policy.

Both students and parents/guardians must read and sign this policy. It should then be returned to your home room teacher.

The purpose of Information and Communication Technologies (ICTs) at St Pauls Catholic College is to:
• Enhance student learning opportunities.
• Promote student achievement.
• Support the professional work of staff.
• Enhance the school's management information and business administration systems.
The use of these ICTs within school should be responsible, legal, appropriate and for educational purposes and should follow the guidelines outlined in this policy. This policy applies to the use of all school related ICTs for educational purposes, whether provided by the school or the student.

Student information - Name, Class, and Email may be given to external providers such as Jacaranda, Cambridge Press, Edmodo and other educational supporting institutions. A copy of each provider Privacy statement is available on their web sites.

Definitions
Information and Communications Technologies are any electronic device or related applications which allow users to record, send, access or receive information, in textual, audio, image or video form. These may include but are not restricted to:
• Computer systems and related applications such as email and Internet.
• Web-based tools such as discussion forums, chat rooms, blogs, pod casts, social networking sites and instant messaging systems.
• Mobile devices such as iPads, mobile phones, PDAs.
• Fax machines.
• Imaging tools such as video or still cameras.
• Audio tools such as audio recording devices.
• CeNet.

Acceptable uses
Students should:
1. Respect resources
• Use ICT equipment and resources for educational purposes under teacher supervision.
• Follow teacher directions for accessing files, programs, email and Internet resources.
• Seek advice from a teacher before responding to online prompts.
• Delete emails from unknown sources without opening any attachments as they may contain a virus.
2. Respect others
• Respect the rights, beliefs and viewpoints of others.
• Follow the same standards of behaviour online as you are expected to follow in real life.
• Follow the Netiquette guidelines for online communications at the end of the document.
• Observe copyright rules by respecting the information, ideas and artistic works of others.

• Acknowledge the author or publisher of information from the Internet and do not claim the work or pictures as your own.

3. Keep yourself safe online

• Keep your passwords and personal work secure.
• Use the Internet and email for educational purposes only.
• Use school provided email accounts when communicating online.
• Seek teacher advice before providing personal details online.
• Always get teacher permission before publishing any personal information or photos online.

Unacceptable uses

The following uses of ICTs are considered unacceptable:

1. Personal safety

Disclosure of personal information can expose users to inappropriate material, physical danger, unsolicited commercial material, financial risks, harassment and bullying, exploitation, unreliable information, nuisance and sabotage.

You should **NOT**:

• Send or post detailed personal information, images or audio about yourself or other people. Personal contact information includes home address, telephone or mobile number, school address, work address, email addresses, etc
• Meet with someone you have met online without your parents/guardian's approval and participation.

2. Illegal activities

Students need to be aware that they are subject to laws relating to assault, trafficking and computer offences.

An electronic audit trail may provide evidence of offences.

You should **NOT**:

• Attempt to gain access to any computer system or service, to which you do not have authorised access. This includes attempting to log in through another person's account or accessing another person's files or emails.
• Make deliberate attempts to disrupt other people's use of ICTs.
• Make deliberate attempts to destroy data by hacking, spreading computer viruses or by any other means.
• Engage in any illegal act, such as threatening the personal safety of others, arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, etc.
• Install or use software which is not licensed by the school.

3. Network security

You should **NOT**:

• Provide your password to another person or in response to a request via email (even if it looks like the email comes from someone you know).
• Go looking for network security problems, because this may be seen as an attempt to gain unauthorised access to the network.
• Post information that, if acted upon, could cause damage to or disrupt the network.
• Open e-mails from unknown sources.
• Download any digital content without express permission of staff.
• Leave the computer while logged onto the network.

4. Inappropriate language

Restrictions against 'inappropriate language' apply to public messages, private messages, and material posted on web pages.

Messages sent using the schools ICTs may be monitored or scanned.

You should **NOT**:

• Use obscene, profane, rude, threatening, sexist, racist, disrespectful or inappropriate language.

5. Respect for privacy

You should **NOT**:

• Re-post a message that was sent to you privately without the permission of the person who sent the message.

•Take photos, sound or video recordings of people, including background figures and voices, without their permission.

• Distribute private information, including photos or recordings, about another person without their permission.

• Send or post any digital content relating to and or identifying the College or Staff without the express permission of the Principal.

6. Respect for others

You should **NOT**:

• Make personal attacks on another person.

• Harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If someone tells you to stop sending them messages, you must comply with their request.

• Send or post any inappropriate or inaccurate information, comments, images, video or audio about other people or organisations.

• Send or post personal information about other people without their permission.

• Send or post any digital content that may be found to be offensive by others.

7. Respecting resource limits

You should **NOT**:

• Use ICTs for other than educational activities and limited, high quality, self discovery activities.

• Download or send large files (>5 Mb) without Teacher permission.

• Post or respond to chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.

• Store any unauthorised material on the College network.

8. Plagiarism and copyright

You should **NOT**:

• Plagiarise works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

•Use material from the Internet in a manner which violates copyright laws.

• Access or use material from the Internet which relates to exam cheating or providing completed assignments.

9. Access to inappropriate material

Attempts to access inappropriate material using the schools ICTs is monitored and logged by the College or the CEO.

Some inappropriate material may be filtered or blocked by the College or CEO.
You should **NOT**:
• Use ICTs to access material that:
  • is profane or obscene (pornography).
  • advocates illegal acts.
  • advocates violence or discrimination towards other people.
• Participate in online chats, discussion groups or mailing lists that are not relevant to your education.
• Access material which is not relevant to your education.
• Use the school ICTs to purchase, order or sell any goods.
A special exception may be made if the purpose of such access is to conduct educational research and both the teacher and the parent/guardian approve access.

10. Mobile Device Policy
PREAMBLE:
Mobile devices provide a number of tools that can be used to support students' learning. This includes the ability to film, photograph, record audio and take notes. As well as this these devices are capable of providing access to the internet. This policy is designed to give teachers and students the opportunity to make the best possible use of available hand held devices to facilitate learning. **The College does not accept responsibility for the loss, damage, theft, or misuse of any mobile device.**

EXPECTATIONS:
Students are able to use their mobile devices at the College as long as they meet the following expectations.
During classes the use of any mobile device **will be directed by the supervising teacher**. Students are expected to have any mobile device on the desk in front of them. The device must be switched to silent unless otherwise directed by the teacher.

The use of any mobile device will be allowed before school, at recess, lunch and after school and it is the students' responsibility to ensure that the device is used appropriately.

INAPPROPRIATE USE
Unless otherwise directed by the supervising teacher students' devices are to be switched to silent and students are not to answer, text or talk using their device in class.

Mobile devices are not to be used in the short break as students move between lessons.

The student is not to use the device to breach anyone's privacy. Filming, photography and audio recordings are only to be made with permission of the supervising teacher and are to be for specific educational purposes.
PLEASE NOTE: the filming of violent incidents is a serious offence and may jeopardise the student's enrolment at the College.

Any use of the device to harass, intimidate, threaten or bully other students or staff will be immediately reported to the Police and may jeopardise the student's enrolment at the College.
PLEASE NOTE: staff have the right to confiscate the phone if it is believed there is evidence related to an incident or incidents of a criminal nature recorded on the phone. This phone will be provided for any Police investigation should this be required.

Mobile devices are not to have offensive ring or message tones. Inappropriate images are not to be used as screen savers and these images should not be stored on any device.

Inappropriate use of the mobile device will lead to the device being confiscated and the privilege of having the device at school withdrawn. This will mean that the device will have to be "checked in" at the student foyer each morning and collected again in the afternoon.

PLEASE NOTE the following expectations apply when students are listening to devices using earphones.
The supervising teacher will use their discretion in deciding whether it is appropriate for a student/s to be listening to a mobile device with earphones. In making this decision teachers will take into account a number of factors including the nature of the work that students are engaged in and the safety of students. These devices are not to be used at any time where their use would compromise safety. Further to this the following expectations apply:
o the College allows the use of earphones but does not accept the use of headphones (earphones sit discreetly in the ear);
o earphones are to be removed for all announcements including daily prayer;
o mobile devices are not to be used, under any circumstances, during homeroom;
o listening with earphones at a high volume damages hearing. People in close proximity to the student listening should not be able to hear what is being played.
o students are encouraged to have their own personal set of earphones. Sharing earphones is not hygienic. Students are discouraged from using this practice.

Notification
You should:
• Disclose to your teacher any messages you receive that are inappropriate or disturb you.
• Notify the IT Dept of the College if you identify a possible security problem.
• Immediately disclose accidental access to inappropriate material to the IT Dept.of the College. This will protect you against an allegation that you have intentionally violated the School Acceptable Use Policy.
• Notify the IT Dept. at the College if you are offended by another person's use of ICT.

Consequences of improper use
Any user violation will be recorded and may be subject to the following consequences:
• Loss of access privileges for a period of time.
• Dealt with in accordance with the College discipline policy according to the nature and severity of the breach.
• Informing parents/guardians.
• Legal action.

Netiquette
Netiquette refers to the guidelines and etiquette for online communication
You should:
• Ensure that email and online messages are written carefully and politely. You should also try to keep messages short and precise.
• Check e-mail frequently and delete unwanted messages promptly.
• Use appropriate language. Anything you post online is public.
• Be cautious in using humour and satire as they can easily be misinterpreted.
• Respect the rights, beliefs and viewpoints of others.
• Follow the same standards of behaviour online as you are expected to follow in real life.
• Ensure Caps Lock is off when typing text, as typing in all capitals is equivalent to online shouting.

Created on 8/12/2016 Student Acceptable Use of ICT Secondary.doc

STUDENT NAME…………………………………………………………………………………….

HOMEROOM……………………………………………………………………………………………

Letter of agreement

Student

I understand and will abide by the above Acceptable Use Policy. I further understand that any violation of the above is unethical and may constitute a criminal offence. Should I commit any violation, my access privileges may be revoked, and disciplinary and/or legal action may be taken.

Name: _____ Date: _____

Signature: _____

(If you are under the age of 18, a parent or guardian must read and sign this agreement.)

Parent or Guardian

As the parent or guardian of this student, I have read the Acceptable Use Policy. I understand that these resources are designed for educational purposes. I also recognise that it is impossible to completely restrict access to controversial materials. I hereby give permission for my child to be given access to information and communication technologies as deemed appropriate by the school, including access to email and the Internet and their information be given to external educational providers as required.

Name: _____ Date: _____

Signature: _____