Introduction
This policy governs the use of all electronic communications and including mobile communication devices, mobile phones and laptops. At Star of the Sea, this policy is grounded in the philosophy of Pastoral Care whereby all members of the school community are treated with dignity, respect and justice, and feel safe and secure. It is also grounded in the philosophy that the education of the whole person is our primary focus.

Rationale
Star of the Sea also recognises that most students now feel the need to carry a mobile phone or other portable communication device. While it is a valuable tool, it must be used responsibly. While Star has positive cybersafety practices, the nature of the internet means that for many students the mobile device also serves as a way to access internet, use educational applications, calendar, address book, camera, watch, diary and for many parents a safety device whereby they can be contacted or used in an emergency.

Rather than banning portable communication devices, Star of the Sea prefers to educate girls in appropriate use, protocols and Privacy and Communication regulations pertaining to such devices.

The use of Information and Communications Technology (ICT) broadens educational horizons and therefore is seen as an integral component of curriculum delivery.

The computer network at Star of the Sea provides a high level of ICT access in a safe and secure environment to facilitate:

- Learning opportunities to enhance all learning domains.
- The development of student confidence and competence in the use of ICT and cyber-citizenship.

As a tool of the learning process ICT enables students to research information from a wide variety of sources, to communicate readily with others and to prepare, redraft and store work. Electronic research and communication skills are part of a portfolio of skills, which students need to become lifelong learners.

Access to electronic communications is a privilege and not a right. Legitimate use is specifically for educational purposes only. These include:

- Research activities as part of the school curriculum.
- Producing work that relates to associated learning activities
- The use of email for exchanging appropriate information and engaging in collaborative projects.
- The authoring of Internet home pages where applicable.
- Consequently, access entails responsibilities which are outlined below.
MOBILE COMMUNICATION DEVICE GUIDELINES

- Mobile phones are not to be used for communication - chat, message, calls to others who are in or outside the school using between 8:30am - 3:20pm.

- Mobile communication devices are not to be used at recess or lunchtime.

- Communication between parents/guardians and students is to be conducted via the Student Services Secretary. Students are not to contact parents/guardians in the event of illness. Students are to report to Student Services if feeling unwell, where parents/guardians will be contacted.

- Students are not to make phone calls during the school day. If they must make a call, they need to seek permission and make the call at the Student Services Office.

- In certain classes devices may be used as learning tool with the express permission of the teacher in the classroom. The use of the device is left to the discretion of the teacher. eg: use of phone as MP3 player with headphones to listen to podcasts or quiet music for focus, audio recording of discussions, note taking, photos of board work. This includes Year 11 Study Hall.

- Mobile communication devices are not be brought into any formal assessment during classes or examinations and may result in having results cancelled (Star of Sea’s protocols are that mobile communication devices are left with the teacher during assessment tasks in VCE Subjects).

- Students and families are advised that mobile communication devices are brought to school at the owner’s risk. No liability will be accepted by the College in the event of the loss, theft or damage of the mobile communication devices unless it can be established that the loss, theft or damage resulted from the school’s negligence.

- Parents and students should record the IMEI code which is located under the battery inside the mobile phone. It can also be displayed on the screen of the phone by entering *#06# into the keypad on most phones. The IMEI number is used by the network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network. For example, if a mobile phone is stolen, the owner can call his or her network provider and instruct them to “ban” the phone using its IMEI number. This renders the phone useless, whether or not the phone's SIM is changed.

- The College will take appropriate action against any student who photographs or films other members of the College community without their consent or who sends harassing, threatening or inappropriate SMS, MMS and email messages.

MOBILE COMMUNICATION DEVICE PROTOCOLS
In the event that a student uses the mobile communication device in an inappropriate way or breaches these guidelines the following protocols will be enacted:

1. 1st incident: Phone confiscated and may be collected at end of the day from Student Services.

2. 2nd incident: Phone confiscated as above and parents notified.

3. 3rd and subsequent incident: Phone confiscated and parents will need to collect their daughter’s phone.
### A. General Computer Use

1. All messages, information and data sent and received using Star of the Sea’s telecommunications network are the property of Star of the Sea.

2. Students use their own password when logging into the network; using another person’s password is not permitted.

3. Using another person’s programmes or data without permission is not permitted.

4. Work must be stored in the space allocated to each student.

5. In line with copyright laws, the work of others must be appropriately acknowledged.

6. Using impolite, abusive or otherwise objectionable language in either public or private documents is prohibited. Using any material that is deemed by the Principal to be against the school’s Catholic ethos is prohibited.

7. Students must not use the ICT in a manner which brings the school into disrepute.

8. Use of ICT must be curriculum related.

9. Software installation on school hardware must be carried out by a member of staff.

10. Students must not vandalize hardware, data or material via the use of the Internet. Students must not upload or create viruses.

11. The network shall not be used for:
   a. Circumventing security measures on school or remote computers or networks, data or material via the use of the Internet.
   b. Downloading and circulating unacceptable or offensive information.

12. Information published on the Internet may be inaccurate or may misrepresent a person or situation. Accordingly students must critically evaluate this information and use with due care and consideration.

### B. Internet

1. Students will not knowingly use the Internet to access, retrieve or distribute material that is deemed offensive according to the Commonwealth Crimes Act Section 85ZE, that is, downloading, distributing or viewing of pornography, racist or other material which degrades another person. This relates to media such as images, videos, words and music.

2. The Internet must not be used to generate or access unacceptable material including Sexually explicit or potentially dangerous material. If unacceptable material is accidentally located, students must notify a staff member immediately.

3. The Internet must not be used for commercial transactions or profit.

4. The school accepts no responsibility for purchases via credit cards or for meeting the requirements of any other contract.

5. The Internet must not be used for political purposes.

6. On line publications e.g. Blogs, Wikis and G pages are formal publications and their contents and use must only be for educational purposes. They will be checked and approved by the appropriate member of staff.

7. Students should not upload images of the school or any other information that identifies the school for their own personal use on the internet without the permission of the Principal. This includes pictures of themselves in school uniform, teachers or images from school events. (Especially on such webspaces such as Facebook, My Space or You Tube). Whilst the list of possibilities is endless, in all matters of concern discretion as to which material is inappropriate rests with the Principal.
C. Communication  
(Including email, mobile phones or social media)

Mobile Communication Devices are a valuable tool for communication. Students should be aware that their school email may be monitored.

Examples of unacceptable use include but are not limited to:

1. Sending or displaying offensive and anti-social material.
2. Using obscene language.
3. Harassing, threatening, insulting or attacking others.
4. Sending messages that result in losses of the recipient’s work or damage the system.
5. Identity theft via mobile phones or social media networks.
6. Using the network to disrupt its use by other individuals or by connecting networks.
7. Disrespect of others’ privacy and intellectual property.
8. Trespassing in the folders or files of others.
9. Using other users’ email addresses and passwords.
10. Using any means to avoid scrutiny by teachers of work in progress.
11. Damaging computers, computer systems or computer networks (for example, by the creation, introduction or spreading of computer viruses, damaging hardware, altering source codes or software settings, etc.)
12. Use of material copied from the internet without acknowledgement.
13. Employing the network for commercial purposes or activities by for-profit institutions or organisations, product advertisement or political lobbying.
14. Sending messages which bring the school into disrepute.
15. Intentionally wasting time or resources.

Consequences of inappropriate use of ICT

Students who do not follow the guidelines for use will, in the first instance, have the matter reported by the staff member to the Deputy Principal – Students and relevant Pastoral Coordinator who will inform the Information Technology Manager. Possible consequences will be directed by the Pastoral Coordinators in consultation with the Deputy Principal - Students and may include:

1. Making a formal apology.
2. Receiving a reprimand.
3. Attending an interview about the offence in the presence of parents.
4. Losing unsupervised access for a prescribed period of time.
5. Suspension from school.
6. Serious incidents may require the College to inform the police.

Any extreme breaches of the policy could lead to consideration of a student’s place in the school. Pastoral Coordinators will take the appropriate action after consultation with the relevant individuals.
INFORMATION AND COMMUNICATIONS TECHNOLOGY: STUDENT AGREEMENT

When using ICT devices I agree to behave according to the Guidelines of this User Agreement.

1. I will use ICT devices at school only during classtime (this includes school related activities and study periods) for educational purposes and only as directed by teachers.

2. I agree that when talking and working with others (including online, messaging and chat) I will use appropriate language and not deliberately harass others. I will not enter or remain in any site that has obscene language or offensive content (e.g. racist material or violent images).

3. I will abide by copyright procedures when using content on websites (ask permission to use images, text, audio and video and cite references where necessary) and think about how I use the content posted on the Internet, and not simply copy and paste information from websites or another student’s work. I will evaluate the legitimacy of online content before utilising it in my work.

4. I will respect the privacy and files of others. I will not interfere with network security, the data of another user, attempt to log onto devices or networks, such as school or social media, with the username or password of another student.

5. I will not bring or download unauthorised software, including games to the school computers.

6. I understand that the school may monitor traffic, stored content and material sent and received using the school’s network. The school may use filtering and/or monitoring software to restrict access to certain sites and email.

7. I will take proper care of school ICT equipment. I know that if I have been involved in the damage, loss or theft of equipment/devices, my family may be responsible for the cost of repairs or replacement.

8. I understand that I am responsible for the security of personal devices brought to school. The College will not be held responsible for the loss of personal devices.

9. I understand that the school may audit and review the student use of its computer network, Internet, hardware and other devices. Such auditing may include any stored content, including email.

10. I will ask permission to use mobile communication devices to record or share audio, video or images of others.

11. I will protect my mobile phone numbers by only giving them to friends and family. (This can help protect a student’s number falling into the wrong hands and guard against the receipt of unwanted or inappropriate calls or messages.) I will protect my privacy rights and those of others by not giving out personal details including account passwords, full names, telephone numbers, addresses and images.
12. I will talk to my teacher or another adult if:
   - I need help online.
   - I feel that the welfare of other students at the school is being threatened.
   - I come across sites which are not suitable for our school.
   - Someone writes something I do not like, or makes me or my friends feel uncomfortable or asks me to provide information that I know is private.
   - If I suspect people are impersonating others via email or social media.

13. I understand that if I break this Use Agreement the school may ban or restrict my ICT use, and/or inform my parents. Consequences may include confiscation of mobile device, meeting with Pastoral Coordinators, myself and my parents, or suspension from the college. I also understand that my parents may be charged for repair costs. If illegal material or activities are involved, it may be necessary for the college to inform the police.

14. I understand that I will follow the guidelines, even outside the school with respect to avoiding actions that are disrespectful to others, myself or the school.

15. I acknowledge and agree to follow these guidelines. I understand that my access to the Internet and mobile technology will be negotiated if I do not act responsibly.
INFORMATION AND COMMUNICATIONS TECHNOLOGY: STUDENT AGREEMENT

Student Commitment

Student Name: ____________________________________________________

Year Level: ___________ Homeroom: ______

Student’s Mobile Number: __________________________________________

Student’s IMEI Number: ____________________________________________

Student’s Signature: ______________________________________________

Date: __________________________

Parent’s Commitment

I have read this User Agreement and am aware of and support the College’s initiatives to maintain a cybersafe learning environment. I am also aware of my child’s responsibilities.

Parent/Guardian Name: ____________________________________________

Parent/Guardian Signature: _________________________________________

Date: __________________________

Please sign and return this page to your homeroom teacher and keep the agreement documents for future reference.