SACRED HEART COLLEGE

Acceptable use of Information and Communication Technology Policy

Context

Sacred Heart College (SHC) acknowledges the increasing use of information and communication technologies as a learning and business tool in schools. SHC celebrates the capacity of the new technologies including mobile communication devices and the use of social media to foster and support positive relationships and various forms of harmony through the promotion of a culture where there is respect for all and where all are invited to search for truth in dialogue.

Information and communications technology is to be used to enhance the quality of human life, whether in an educational, social, recreational or work context. At the school, technology is mostly used to support teaching and learning and for business purposes. SHC expects technology to be used in a safe, responsible, respectful and ethical manner at all times.

1. Scope

This document is designed to promote the acceptable use of electronic information and communications technology by all students and Workplace Participants.

The document covers the:

- use of SHC ICT Facilities (whether within or outside of normal working hours, and whether on or off site), including use of SHC networks/internet connections to access the internet using Personal ICT Devices (whether within or outside of normal working hours), and including remote access
- other use of Personal ICT Devices (including outside of normal working hours and including when off-site) where such use:
    - is likely to cause serious damage to the relationship between SHC and the student or Workplace Participant or
    - is likely to damage the interests of SHC or
    - is incompatible with the student's or Workplace Participant's duty to SHC.

2. Responsibility for implementation, monitoring, and continual improvement

3.1 Responsibilities of all Students and Workplace Participants

3.1.1 The use of SHC ICT Facilities (including the use of Personal ICT devices to access material on the Workplace's network and services) should be consistent with the Catholic ethos and the values espoused by Marist Schools Australia. Any reference to Catholicism, Catholic Church, Catholic schools, Pope, the Bishop and other clergy must be consistent with obligations to uphold the Catholic ethos.

3.1.2 In using the SHC ICT Facilities or Personal ICT devices that access material on the Workplace's network and services, students and Workplace Participants must:

- behave ethically and responsibly in all dealings with others
- observe obligations regarding confidentiality and privacy
- maintain a secure password and ensure that they do not provide the password to anyone else

- not attempt to gain unauthorised access to anyone else's account or user information, or otherwise attempt to defeat any security controls
- not use another person's email account or other means of communication to send any communication in that other person's name (unless specifically authorised by that person)
- not take photos or video of members of the school community without their consent
- ensure that they do not permit or facilitate unauthorised use of the SHC ICT Facilities by anyone
- promptly report any evidence or reasonable suspicion of unauthorised access/use to SHC authorities and
- promptly report any accidental access to inappropriate material.

3.1.3 SHC ICT Facilities or Personal ICT devices that access material on the Workplace's network and services should not be used to:

- send or publish any statement, image or other material that is offensive or threatening, or could constitute harassment, discrimination, vilification, defamation or cyberbullying
- knowingly access, download, store, send or publish any material that is pornographic
- do anything that the user knows or reasonably suspects could contravene the law, including without limitation downloading material in breach of copyright
- send or help to send unsolicited bulk email (spam)
- open or download any attachment, or access any link, that the student or Workplace Participant reasonably suspects may contain a virus, malware or other computer contaminant (any such attachment or link should be forwarded to the Workplace ICT personnel for authentication)
- obtain unauthorised access to the SHC or any other network, or to deliberately degrade the performance of the SHC data network or
- install any unlicensed or non-approved software onto computers or other communication devices supplied by SHC

4.1.4 Students and Workplace Participants are responsible for the physical control and safe keeping of any laptops, mobile telecommunication devices, and other communication devices supplied to them by SHC, and are responsible for ensuring that other people do not access any confidential information contained on the device, or misuse the device.

4.1.5 Students and Workplace Participants may use SHC ICT Facilities for incidental personal use, provided such use is minimal and does not interfere with the performance of their studies/duties, but are not permitted to use SHC ICT Facilities to store or download large files (including music or movies) for personal use. All personal use of SHC ICT Facilities must conform to this practice.

4.1.6 Personal devices that access material on the Workplace's network and services must be protected with a secure password, access code, pattern or PIN

4.1.7 Where a device that contains SHC data is lost or stolen SHC authorities reserve the right to erase all data on the device including any personal data.

4.1.8 Student's and Workplace Participants' use of SHC ICT Facilities (including Personal ICT devices that are used to access material on the Workplace's network and services) may be monitored by SHC ICT personnel, and any evidence of use that contravenes this practice, or is otherwise inappropriate, may lead to disciplinary consequences.

4.1.9 When posting material in a Social Media forum (eg Facebook page, Twitter, blogs) students and Workplace Participants should be aware that such activity may be considered public, not private.

4.1.10 If someone else posts a comment or other material in a student or Workplace Participant's Social Media space, then if that comment or material:

- is likely to cause serious damage to the relationship between SHC and the student or Workplace Participant or
- is likely to damage the interests of SHC or
- is incompatible with the student or Workplace Participant's duty to SHC,
- the student or Workplace Participant must (where possible) remove that comment or material as soon as it comes to their attention.

4.1.11 Student and Workplace Participants accessing a public network (Internet) not managed by SHC must comply with this Acceptable Use practice.

4.2 Responsibilities of Principals

The additional responsibilities of Principals in relation to ICT Acceptable Use are to:

4.2.1 implement appropriate measures in his or her School to enable compliance with these practices to be monitored, and to enable any breaches to be detected

4.2.2 ensure that on an annual basis, promptly at the commencement of each school year, his or her School prepares and implements an Acceptable Use Agreement incorporating all of the matters set out in the Appendix

4.2.3 encourage participation of students, parents and staff in the preparation of the Acceptable Use Agreement

4.2.4 ensure that all Workplace Participants and students (and parents in the case of students under the age of 18 years) sign the Acceptable Use Agreement at the beginning of each school year (or when the Workplace Participant or student joins the school, if part-way through the year)

4.2.5 ensure appropriate storage of the Acceptable Use Agreements

4.2.6 ensure regular professional development sessions are conducted and informal reminders are issued to Workplace Participants in relation to the school's Acceptable Use Agreement and Acceptable Use Policy, and that new Workplace Participants are made aware of the Acceptable Use Policy and the Acceptable Use Agreement as part of their induction process

4.2.7 ensure regular information and education sessions are held for students (and where appropriate, parents) to promote understanding of available technologies, the inherent risks involved in use of those technologies, and the content of the Acceptable Use Agreement

4.2.8 promptly report to the Principal Consultant (and Marist Schools Australia) any known or suspected breaches of the school's Acceptable Use Policy and Acceptable Use Agreement that may constitute a criminal offence.

4.3 Additional Responsibilities of School staff

4.3.1 Workplace Participants are required to educate students about the use of technology and the risks involved in that use, including the potential inaccuracy of online information, ways to check the authenticity of information, and strategies to stay safe online

4.3.2 Workplace Participants are required to work with the Principal to implement regular information and education sessions for students (and where appropriate, parents) to promote understanding of available technologies, the benefits of, and inherent risks involved in, use of those technologies, and the content of the Acceptable Use Agreement

4.3.3 Workplace Participants are required to promptly report to the Principal any known or suspected breaches of the school's Acceptable Use Policy and Acceptable Use Agreement that may constitute a criminal offence.

4.3.4 When using the SHC ICT Facilities or Personal ICT devices that access material on the Workplace's network and services, Workplace Participants must only obtain access to records or information that is relevant their duties and have been authorised to access

4.3.5 Workplace Participants are required to promptly report to SHC authorities any loss of, or unauthorised access to, any communication devices that contain work-related information or information that is otherwise confidential to SHC.

4.3.6 Upon conclusion of their role within SHC, Workplace Participants must permanently remove from their Personal ICT Devices any work-related information, or information that is otherwise confidential to SHC.

4.3.7 Workplace Participants must not:

- connect or interact with students through Social Media (eg Facebook friends or Facebook private messages) without the Principal's written consent, other than in the case of any Social Media site specifically created or provided by a School (and authorised by the Principal) for the purpose of facilitating online communication between Workplace Participants and students; or
- divulge any confidential information, including students' personal information, through Social Media.

4.3.8 Workplace Participants' use of SHC ICT Facilities (including Personal ICT devices that are used to access material on the Workplace's network and services) may be monitored by SHC ICT personnel, and any evidence of use that contravenes this practice, or is otherwise inappropriate, may lead to disciplinary consequences in accordance with section 4.4 Consequences of Non-Compliance. In the case of an investigation into the conduct of a Workplace Participant, the Workplace Participant must, if requested, provide his or her Personal ICT devices to SHC authorities (together with any information such as passwords that is necessary to gain full access to the devices) for the purposes of assisting the authorities to determine whether inappropriate conduct has occurred.

4.4 Consequences of Non-Compliance

In the event that a student is found to have breached the Acceptable Use Policy or Acceptable Use Agreement, consequences that may result will be in accordance with the current disciplinary practices.

In the event that a Workplace Participant is found to have breached the Acceptable Use Policy or Acceptable Use Agreement, consequences may include:

- verbal counselling or warning
- written counselling or warning
- formal final warning or
- dismissal

as well as limitation or suspension of some or all of the Workplace Participant's right to use SHC ICT Facilities.

Any investigation will be carried out in accordance with the SACCS 2005 document: Procedures for Dealing with Allegations of Misconduct.

Evidence of illegal conduct by students or Workplace Participants will be reported to SAPOL or the Australian Federal Police (as appropriate).

4.5 Conclusion

The terms of this document are not intended to be exhaustive, nor do they anticipate every possible use of SHC's ICT Facilities. Students and Workplace Participants are encouraged to act responsibly and take into account the principles underlying ICT Acceptable Use.

5 Definitions

SHC ICT Facilities - include computer systems, cloud based resources, data networks, wireless infrastructure, internet connections, computers, laptops, smart phones, other devices, applications and printers and other means of electronic communication provided by the Workplace.

Cyberbullying - is the use of the Internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner.

Personal ICT Device - means a device owned, leased or otherwise used by an individual that is not provided by the employer but is capable of accessing material on the Workplace's network and services, or is capable of acting as a Wifi hotspot.

SHC – means Sacred Heart College

SHC authorities – are the members of the Senior School Leadership Team, Middle School Leadership Team, or the College Executive.

Social Media - refers to a range of online services and tools used for publishing, sharing and promoting interaction and dialogues.

Workplace - means Sacred Heart College in the case of Workplace Participants working or volunteering.

Workplace Participants – means employees, consultants, contractors, volunteers and guests of Sacred Heart College.

6 Related documents/links

- The following documents are to be read in conjunction with this Policy.
- SACCS Information and communications Technology Security Policy
- SACCS Information and communications Technology Security Framework
- SACCS 2005 document: Procedures for Dealing with Allegations of Misconduct.

Policy Title	Acceptable use of Information and Communication Technology Policy
Ratified by Executive and College Council	February 2019
Policy due for review	February 2022

[To be signed by student and parent/caregiver at time of enrolment (most often by students entering Year 6)]

STUDENT USER AGREEMENT

Sacred Heart College

This User Agreement sets out the terms on which you may access ICT facilities provided by Sacred Heart College (SHC) and cloud computing services, including Edumate and Google Apps for Education (GAFE). Cloud computing involves the use of web-based services (rather than a PC or school server) for functions such as email, blogs, lodgement of assignments and data storage.

You will need to sign and return this User Agreement before you will be allowed to access these Services.

By signing this User Agreement, you (including parents/guardians in the case of students under 18 years) are agreeing to the terms set out in this User Agreement, including the consequences of any breach of the terms.

1. Privacy Consent

Information that you transfer or store using the school's Cloud Computing Services (including email, assignments, blogs and data storage) may be stored by Edumate and Google Apps for Education (GAFE) in the United States of America, or such other country as the Cloud Providers may decide. By using the school's Cloud Computing Services, you are consenting to the transfer to, and processing and storage of your information in, such overseas location, even though the privacy laws in those countries may be different to the privacy laws in Australia.

2. Acceptable Use

You agree that you will comply with all requirements as set out in this Agreement and in the Acceptable Use Policy and all other relevant laws and restrictions in your access to the various information and communication technology resources through the SHC network (including email, the Internet, cloud computing services and services provided through third parties), that you will not use the Cloud Computing Services to do anything that is against the law, and that you will not:

(a) send or help to send unsolicited bulk email (spam);

(b) publish material that is hurtful or offensive to other people, including material that is defamatory, threatening or discriminatory;

(c) knowingly create or send any viruses, worms, Trojan horses or anything of a similar nature; or

(d) disable, change, reverse-engineer or otherwise interfere with the Cloud Computing Services;

(e) Students are required to obtain teacher permission prior to establishing contact with participants not associated with their school.

3. Monitoring

You agree that school Workplace Participants are responsible for ICT systems will have the ability to (and may at any time) monitor your use of the Cloud Computing Services, including accessing and monitoring any data that you have sent or stored using the Cloud Computing Services, to ensure that you are using the Cloud Computing Services appropriately.

4. Suspension or termination of use and other consequences

If there is an emergency security issue, or if you are suspected of making inappropriate use of the Cloud Computing Services, your access to the Cloud Computing Services may be suspended or terminated. This means that you might not be able to access your school email, assignments, blogs and data storage. If you are found to have made inappropriate use of the Cloud Computing Services, the school may also apply other disciplinary consequences.

Agreement and Consent

I, the student named below hereby agree to comply with all requirements as set out in this Agreement and in the Acceptable Use Policy and all other relevant laws and restrictions in my access to the various information and communication technology resources through the SHC network (including email, the Internet, Cloud Computing Services and services provided through third parties).

NAME: _____ CLASS: _____

SIGNATURE: _____ DATE: _____

Parent/Guardian Consent (for students under 18 years of age)

As the parent or legal guardian of the student named above, I consent to the student accessing the various information and communication technology resources through the SHC network (including email, the Internet, Cloud Computing Services and services provided through third parties) on the terms set out in this Agreement and in the Acceptable Use Policy and all other relevant laws and restrictions.

NAME: _____ DATE: _____

SIGNATURE: _____

Appendix B – Workplace Participants Acceptable Use Agreement.

[To be signed by Workplace Participant at time of employment induction]

Workplace Participants USER AGREEMENT

Sacred Heart College

This User Agreement sets out the terms on which you may access ICT facilities provided by Sacred Heart College and cloud computing services, including Edumate and Google Apps for Education (GAFE). Cloud computing involves the use of web-based services (rather than a PC or school server) for functions such as email, blogs, lodgement of assignments and data storage.

You will need to sign and return this User Agreement before you will be allowed to access these Services.

By signing this User Agreement, you (including parents/guardians in the case of students under 18 years) are agreeing to the terms set out in this User Agreement, including the consequences of any breach of the terms.

1. Privacy Consent

Information that you transfer or store using the school's Cloud Computing Services (including email, assignments, blogs and data storage) may be stored by Edumate and Google Apps for Education (GAFE) in the United States of America, or such other country as the Cloud Providers may decide. By using the school's Cloud Computing Services, you are consenting to the transfer to, and processing and storage of your information in, such overseas location, even though the privacy laws in those countries may be different to the privacy laws in Australia.

2. Acceptable Use

You agree that you will comply with all requirements as set out in this Agreement and in the Acceptable Use Policy and all other relevant laws and restrictions in your access to the various information and communication technology resources through the SHC network (including email, the Internet, cloud computing services and services provided through third parties), that you will not use the Cloud Computing Services to do anything that is against the law, and that you will not:

(f) send or help to send unsolicited bulk email (spam);

(g) publish material that is hurtful or offensive to other people, including material that is defamatory, threatening or discriminatory;

(h) knowingly create or send any viruses, worms, Trojan horses or anything of a similar nature; or

(i) disable, change, reverse-engineer or otherwise interfere with the Cloud Computing Services.

3. Monitoring

You agree that school Workplace Participants responsible for ICT systems will have the ability to (and may at any time) monitor your use of the Cloud Computing Services, including accessing and monitoring any data that you have sent or stored using the Cloud Computing Services, to ensure that you are using the Cloud Computing Services appropriately.

4. Suspension or termination of use and other consequences

If there is an emergency security issue, or if you are suspected of making inappropriate use of the Cloud Computing Services, your access to the Cloud Computing Services may be suspended or terminated. This means that you might not be able to access your school email, assignments, blogs and data storage. If you are found to have made inappropriate use of the Cloud Computing Services, the school may also apply other disciplinary consequences.

5. Process and Storage of Certain Record

You must not, without the specific written consent of the school Principal, use the Cloud Computing Services for the long term or permanent storage or retention of any of the following school records:

(a) taxation records including records relating to payroll tax and fringe benefits tax;

(b) employee records under applicable industrial legislation;

(c) workers compensation records;

(d) medical records;

(e) records relating to occupational health, safety and welfare laws (including occupational health, safety and welfare policies and procedures and any documents relating to injuries suffered in the course of employment); and (f) school attendance records.

Agreement and Consent

I, the student named below hereby agree to comply with all requirements as set out in this Agreement and in the Acceptable Use Policy and all other relevant laws and restrictions in my access to the various information and communication technology resources through the SHC network (including email, the Internet, Cloud Computing Services and services provided through third parties).

NAME: _____

SIGNATURE: _____ DATE: _____

Appendix C – Chromebook Acceptance form

[To be signed by student and parent/caregiver when transitioning to Senior School (most often by students entering Year 10)]

Chromebook ACCEPTANCE FORM

Sacred Heart College

Students will not be issued a College provided Chromebook until the student and parent/and Caregivers have signed and returned this Acceptance Form to the College.

Student:

I have read the Student Acceptable Use Agreement and the Chromebook User Handbook and I agree to comply with these rules. I further understand that violation of the agreement and/or rules may result in the revocation of computer privileges and may also be subject to further disciplinary and/or legal action.

I further agree that the College issued Chromebook will be issued for my use until my graduation from the College when it must be returned. If my enrolment is terminated by the Principal (or delegate) or if I leave the College for any reason, I agree that I must return the Chromebook.

NAME: _____

SIGNATURE: _____ DATE: _____

Parent/s and Caregiver/s:

I/We have read the Student Acceptable Use Agreement and the Chromebook User Handbook. I/We understand that my son/daughter's use of school ICT equipment/devices is subject to compliance with these rules. I further understand that violation of the policy and/or rules may result in the revocation of computer privileges and may also be subject to further disciplinary and/or legal action.

I/We also understand that we are accepting responsibility for any deliberate or wilful damage, destruction or loss of the issued Chromebook.

I/We further agree that the College issued Chromebook will be issued for my son/daughter's use until my son/daughter's graduation from the College when it must be returned. If my son/daughter's enrolment is terminated by the Principal (or delegate) or if my son/daughter's leave the College for any reason, I/We agree that I/We must return the Chromebook.

NAME: _____

SIGNATURE: _____ DATE: _____