Cyber-safety Guidelines

Introduction
Learning and teaching at St Joseph's Catholic College (SJCC) emphasises the development of 21st century learning skills such as critical and creative thinking, problem solving, working collaboratively and working independently. To assist this learning, teachers and students utilise and apply contemporary information and communication technologies to access, create and communicate information and ideas, solve problems, work collaboratively and perform the multitude of administrative tasks required in a contemporary secondary school.

Purpose
"*Let us boldly become citizens of the digital world… The revolution taking place in communications media and in information technologies represents a great and thrilling challenge; may we respond to that challenge with fresh energy and imagination as we seek to share with others the beauty of God*." (Pope Francis 48th World Communications Day Communication at the Service of an Authentic Culture of Encounter)

When using information and communication technologies, staff and students are expected to conduct their activities in a manner that supports and advances the mission of Catholic schooling in the Diocese and the education and formation of students in Catholic discipleship, and shows respect for the dignity, rights and privacy of all persons. The Diocesan Pastoral Care Policy encourages relationships that are grounded in love, compassion, reconciliation and justice. In witnessing Christian values the St Joseph's community rejects ideas, beliefs and behaviours which marginalise or victimise people.

These guidelines underpin the *Cyber-Safety Guidelines for Systemic Schools in the Diocese of Broken Bay* and are designed to create and maintain a cyber-safety culture in which information and communication technologies are used safely and responsibly to enhance learning, collaboration, relationships and administration. However, some online behaviours are illegal and breach Commonwealth (*The Commonwealth Criminal Code Act* 1995 Section 474.17) and NSW state laws (*The Crimes Act 1900* NSW s 60E, *Crimes (Domestic and Personal Violence) Act 2007 NSW* ss 8, 13.). The college is obligated to report such behaviours to the police.

Cyber-safety issues
Cyber-safety refers to appropriate and responsible behaviour online. It covers the time spent online, online privacy and information protection, good manners and behaviour, respectful communication and knowing how to get help with online issues.

Cyber-safety is an important issue at SJCC because students spend a significant proportion of their time inside and outside school using ICT and from 2018 all students will have their own laptop. Excessive use can have a negative impact on sleep patterns, study, class work, outdoor activity and family relationships especially if students are not open and honest with parents about the nature and extent of their online activities.

In addition there are a number of online safety issues which pose threats to students' emotional lives and thus their ability to learn and conduct normal relationships with family and friends.

Cyber-safety issues students are likely to encounter online include:

- *Unwelcome websites* - often encountered when students search for information utilising internet search engines such as Google, AltaVista etc. These websites often contain material that may be age inappropriate, sexually explicit, pornographic, violent and offensive.
- *Stranger Danger* - where a student is targeted online by a stranger possibly pretending to be someone other than who they really are, intent on establishing a 'trusting' inappropriate relationship before possibly arranging a face-to-face meeting.
- *Cyber-bullying* - occurs when information and communication technologies are used to support repeated and deliberate hostile behaviour intended to harm others such as pranking, teasing, spreading rumours, creating hate sites, making fun of someone, threats, and exclusion from social circles. This can have devastating effects on the victim. SMS/MMS/Mobile carriages may be vehicles for cyberbullying. At St Joseph's the college is committed to reducing and responding to all forms of bullying including cyber-bullying.
- *Sexting* – sending or posting provocative or sexual photos, messages or videos online. People of any age, who forward or share images of a sexual nature of a person under 18 need to be aware that this is a criminal offence (child pornography) that may result in prosecution.
- *Financial exploitation* - made possible through the harvesting of personal information that may include credit card and mobile phone account details through the use of cleverly disguised websites and other downloaded programs e.g. Trojans and viruses.
- *Identity theft* – fraudulently assuming a person's private information for personal gain. Students are exposed to these risks because they are not aware of the extent of their digital footprint and do not take the necessary precautions to protect their private information.
- *Unlawful use* - may arise through the misuse of the Diocesan Schools System Network. Some examples of this may include the downloading and distribution of mp3 and movie files through Peer to Peer networks.

Response to cyber-safety issues

The Catholic Schools Office and SJCC work in partnership to develop security and technical controls, policies and guidelines and education responses to minimise risks associated with learning, cyber-bullying and administrative functions in the digital age.

Security and technical controls

- *To minimise the risks from viruses and intrusions*, current virus screening software is activated and where appropriate, passwords are used by staff and students. Firewalls are maintained and system protocols and server configurations are managed by designated DSS staff.
- *Central content filtering* is provided for all diocesan schools by the Catholic Education
- Network (CEnet). This level of filtering utilises a database of over 20 million blockable websites in over 91 categories.
- *School-based content filters* that provide the technical capacity to block access to sites based on category and/or web address as well as the capability to filter email reception.
- *School-based Internet and email monitoring* to track network traffic, websites visited and web searches conducted for evidence of inappropriate use.

Policies and guidelines

- *Email protocols* that include a signature block at the bottom of e-mail messages stating the author's name, school phone number and postal address and an e-mail disclaimer if the email message does not officially represent the school or the CSO.
- *The creation of websites and online learning communities* using social media platforms will be approved by the Principal when they facilitate the creation and communication information and ideas, solving problems, working collaboratively and

the performance of administrative tasks. Online learning communities established by a SJCC teacher will have another teacher (usually the KLA Leader of Learning) with full administrator access who actively and regularly monitors all activity.

- *Information sheet for students, parents/carers and staff* provided each school year. Refer to Appendix 1.
- *The Student Internet Access Agreement* is signed by students and their parents/carers at the beginning of the school year. New students complete this agreement on enrolment. This agreement is located in the student planner.
- The document *Statements – Use of the Internet and Network Services by DSS staff* is provided to all teaching and office staff each school year. Refer to Appendix 2
- *A Record of all Cyber-safety incidents* brought to the attention of and managed by Year Leaders and breaches of the *Student Internet Access Agreement* identified are maintained.
- Additional resources can be located in Appendix 3.
- *Related legislation, policies and guidelines* that support teachers and students using and applying contemporary information and communication technologies for learning and teaching including:

  Comm. and NSW legislation - Classification (Publication, Films and Computer Games) Act 1995 (Comm.)
  Copyright Act 1968 (Comm.)
  Copyright Amendment [Digital Agenda] Act 2000 (Comm.)
  Privacy Amendment (Private Sector) Act 2000 (Comm.)
  Anti-Discrimination Act 1977 (NSW)
  Children and Young Persons (Care and Protection) Act 1998 (NSW)
  Crimes Act 1900 (NSW)
  Defamation Act 2005 (NSW)
  Workplace Surveillance Act 2005 (NSW)
  Privacy Act 1988 (Comm.)
  Spam Act 2003 (Comm.)
  Enhancing Online Safety for Children Act 2015 (Comm.)

  CSO policies and guidelines - Acceptable Use Policy for Internet/Intranet & Network Services in DSS
  Social Media Policy
  Privacy Policy
  Complaint Handling Policy

  SJCC policies and guidelines -Positive Behaviour for Learning and Teaching Guidelines
  Pastoral Care and Student Wellbeing Policy
  Anti-bullying Policy
  Mobile Phone Use Policy

Education responses

Cyber-safety curriculum units in English and PDHPE and in the Pastoral Care and Student Wellbeing Program

Pastoral care Program – incorporating units on cyberbullying: Brainstorm Productions

School Liaison Police have a strong connection with the school making presentations on cyber-safety issues to year groups and educating and advising small groups and individual students involved in inappropriate online behaviour.

Cyber-safety education for parents with regular features in Joey's Journal about online threats, the different social media platforms, how students are currently using ICT and references to a wide range of education and support websites to assist parents.

Professional learning for teachers

Appendix 1

INFORMATION SHEET FOR STUDENTS, PARENTS/CARERS AND STAFF

The Diocesan School System (DSS) provides access to the internet and network services for students in the belief that digital information and communication environments are important mediums supporting learning, teaching and administration. In using and managing internet and network services students are expected to conduct their activities in a manner that respects the Catholic Church, its mission and its values, and respects the dignity, rights and privacy of other persons.

St Joseph's Catholic College considers that the following uses of the internet and network services by students to be unacceptable:

System Requirements

- Any uses that breach existing Diocesan School System policies.
- Any use that contravenes the ethos and values of the Catholic school system.
- Any attempts to injure the reputation of or cause embarrassment to schools or the Diocesan School System.
- Any use of DSS ICT systems for business or personal financial benefit.
- Any use of DSS ICT systems for party political purposes.

Personal Safety

- Posting of personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, work address, email addresses, etc.
- Meeting with someone they have met on-line without their parent/carer approval and participation.
- Not disclosing to their teacher, any messages they receive that are inappropriate or that make them feel uncomfortable.

Unlawful Use

- Engaging in any illegal act, engaging in any criminal activity, threatening the safety of people, etc.

Privacy Issues

- Posting private information about another person.
- Re-posting a message that was sent to them privately without the permission of the person who sent them the message.
- Sending items of a sensitive or confidential nature by e-mail without prior clarification with the addressee.

Copyright and Plagiarism

- Not respecting the rights of copyright owners: copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.
- Plagiarising 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.

Access

- Attempting to gain unauthorised access to the service or to any other computer system through the service, or go beyond their authorised access. This includes attempting to log in through another person's account or access another person's files.

Inappropriate Use

- Using 'Inappropriate Language' in public messages, private messages, and material posted on Web pages.
- Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- Engaging in personal attacks, including bullying, prejudicial or discriminatory attacks.
- Harassing another person. Harassment is any behaviour that is not asked for and not wanted and that offends, upsets, humiliates or intimidates another person. If a user is told by a person to stop sending messages, they must stop.
- Knowingly or recklessly posting false or defamatory information about a person or organisation.
- Using the service to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people.
- Attempting to access sites and games that are inappropriate in school settings. These include violence, hate and horror sites and games.
- Failing to immediately disclose inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated the School Acceptable Use Policy.

Network Security

- Making deliberate attempts to disrupt the service performance or destroying data by spreading computer viruses or by any other means.
- Intentionally spreading computer viruses.
- Providing their password to another person for accessing services.
- Interfering with the operation of anti-virus software or other computer system security features.
- Altering system files, system configurations, folders and other technical data.
- Not notifying the school network administrator if they have identified a possible security problem or malfunction. However students will not go looking for security problems, because this may be construed as an unauthorised attempt to gain access.

Resource Limits

- Using the services for other than educational or career development activities.
- Downloading or sending large files unnecessarily.
- Using ICT systems in such a way as to impede the efficiency of other users.
- Posting chain letters or engaging in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
- Not checking e-mail frequently nor deleting unwanted messages promptly.
- Subscribing to on-line services or group mail lists that are not relevant to their education or professional/career development.

Monitoring

Students and parents are advised that use of the school's computers and internet and network services may be monitored to:

- Protect against unauthorised access,
- Ensure that systems and networks are functional, and
- Ensure that use complies with this policy and the requirements of the Catholic Schools Office.

Appendix 2

USE OF THE INTERNET AND NETWORK SERVICES BY DIOCESAN SCHOOL SYSTEM STAFF

The following statements are provided to give staff guidance on acceptable and unacceptable uses of Diocesan School System (DSS) internet and network services by employees, contractors and volunteers. These statements supplement information provided in Information sheet for students, parents/carers and staff.

Primary Use

- The DSS internet and network services are educational and administrative tools to be used primarily for those purposes. They must be used lawfully, professionally and appropriately.

Personal Use

- The DSS recognises that staff have family and personal needs that may occasionally require use of the DSS's ICT systems. Such personal use shall be reasonable, brief and not interfere with the performance of work.
- Personal use of ICT systems is subject to all the requirements of school and system policies.

Duty of care

- Schools and systems have a duty of care in preventing harm to students. This duty of care includes protection from obscene and other offensive material.
- Staff must therefore exercise this duty of care in supervising students.

Unlawful Use

- All information stored in and transmitted on DSS computer systems is subject to the provisions of legislation, including anti-discrimination, child protection, defamation and sexual harassment.
- Electronically stored and transmitted documents (which includes email) are "discoverable documents" and can be subject to subpoena.
- Staff may not access, store or transmit unlawful material using DSS internet and network services.

Privacy Issues

- DSS internet and network services must be used in accordance with the *Privacy Act (Comm.).*
- Staff must take reasonable steps to protect information held from misuse and unauthorised access. Therefore, all staff must take responsibility for the security of the ICT provided for their use, not allowing them to be used by unauthorised persons.
- All staff are to deal with private or sensitive personal information according to the *Privacy Policy for Diocesan Systemic Schools*, Diocese of Broken Bay.

Copyright, Plagiarism & IP

- All uses of the DSS internet and network services must be comply with the *Copyright Act 1968 (Comm.)*
- The DSS is the owner of copyright in all material created by its staff in performing their duties.
- Usage and content of the DSS computer systems is subject to the same restrictions as all other intellectual property.
- All data stored on DSS ICT systems is the property of the DSS.

Inappropriate Use

Internet and Network services are provided to staff primarily for their use in the course of employment. Reasonable limited use is available during a staff member's own time provided they are mindful that the resource is primarily provided to support teaching and associated activities. Staff are discouraged from participating in social networking sites except where the service fulfils an education or administrative function. Staff may not use

DSS computers or network services to:

- Engage in personal attacks, including bullying, prejudicial or discriminatory attacks.
- Knowingly or recklessly post false or defamatory information about a person or organisation.
- Access sites and games that are inappropriate in both workplace and school settings. These include violence, hate and horror sites and games.

On DSS ICT or internet and network services staff must not:

- Use 'Inappropriate Language' in public messages, private messages, and material posted on Web pages.
- Use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- Use the service to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people.
- Attempt to access sites and games that are inappropriate in school settings. These include violence, hate and horror sites and games.
- Fail to immediately disclose inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated the School Acceptable Use Policy.

Resource Limits

Staff are required to check their e-mail frequently and to delete unwanted messages promptly.

Monitoring

- The DSS recognises and respects the privacy of staff but reserves the right to monitor and audit content and usage of its computer systems, in order to efficiently and effectively implement its vision, strategies and plans. Staff need to be aware that monitoring and auditing will disclose details of sites visited.
- Disclosing inadvertent access of inappropriate sites to the system administrator or designated supervisor will protect staff against an allegation that they have intentionally violated the Acceptable Use Policy.

Appendix 3

Useful resources:

- The Safe Schools Hub is a one-stop shop for information and resources underpinned by the National Safe Schools Framework. The Hub assists school communities to nurture student responsibility and resilience, build a positive school culture, foster respectful relationships and support students who are impacted by anti-social behaviour, including bullying and cyberbullying.

- The Cyber-safety Help Button is a **FREE** downloadable resource providing a one-stop-shop for cyber-safety information. The Help Button is easy to install and use, and can be downloaded onto computers and mobile devices. Users have the option to **TALK** to someone about online issues that are of concern, **REPORT** inappropriate online content or behaviour, and **LEARN** about good cyber-safety practices.

- The Easy Guide to Socialising Online provides information about the cyber-safety features of different social networking sites, search engines and online games. It provides clear, step-by-step instructions on how to adjust privacy settings as well as site specific advice on how to report cyberbullying, abuse and inappropriate content.