St Joseph's School Tranmere

Information and Communication Technology Policy

Contents

1   Introduction

The South Australian Commission for Catholic Schools (SACCS) acknowledges the increasing use of information and communication technologies as a learning and business tool in schools. SACCS 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. SACCS encourages communities to develop reflective and responsible practices around their use of electronic technologies and the internet.

2   Policy Statement

This Information Communications and Technology Policy articulates responsible behaviours and attitudes when using ICT reflecting our school ethos.

This policy outlines the responsibilities for all members of the school community [staff, parents/caregivers, volunteers, visitors] and students. It includes the use of the computer network, internet facilities and all school or personal digital media devices, including computers, tablets, cameras, mobile phones, portable music players, data storage devices and gaming devices.

The school's information and communications technologies include the utilisation of any employer equipment, property or resource at any time, and includes the use of remote access facilities.

3   ICT as a Transforming Technology for Teaching and Learning

Communication enabled by the use of ICT can facilitate the relationship between the family, the school, and the community, and provide new opportunities for parents and care givers to engage with teachers, learning programs, and their children's progress.

21st century education integrates Information and Communication Technologies, engaging students in ways not previously possible, creating new learning and teaching possibilities, enhancing achievement and extending interactions with local, national and global communities.[2]
[2]Ideas contained in this paragraph are drawn from the MCEETYA (Ministerial Council on Education, Employment, Training and Youth Affairs), "Contemporary Learning: learning in an online world", Victoria 2008, p4

Educators can use ICT to:
- empower students to purposefully select creative activities, applications and modes of communication using visually appealing presentation tools
- provide communication and collaboration tools such as chat, email, messaging, discussion forums, online meetings and video conferencing
- present opportunities for students to be part of broader communities
- make learning activities, information and feedback available online anywhere – anytime
- offer students immediate feedback on their learning queries and progress
- increase parent access to student work and achievement.

Effective integration of ICT can improve pedagogies by empowering educators to:
- connect with and learn from colleagues and students and participate in professional learning programs and collaborative projects
- evaluate, create and share online learning resources with colleagues and shape the development of resources and products.

4 Responsibility for Implementation, Monitoring, and Continual Improvement

In Catholic schools guidelines and codes of conduct for the care, wellbeing and protection of children and young people require honest, respectful and trusting relationships between adults, young people and children.

Responsibilities of all members of the St Joseph's School Tranmere community (including employees, parents/carers, students and volunteers):

. 4.1.1 The use of St Joseph's School Tranmere ICT Facilities (including the use of Personal ICT devices to access material on the school's network, services and any ICT related platform) should be consistent with the Catholic ethos and the values espoused by Catholic Education South Australia.

. 4.1.2 In using the St Joseph's School Tranmere ICT Facilities or Personal ICT devices that access material on the school's network and services, school community members must:

   . behave ethically and responsibly in all dealings with others
   . only obtain access to records or information that is relevant to their duties and that they have   authorisation to access
   . observe obligations regarding confidentiality and privacy
   . maintain a secure password and ensure that they do not provide the password to anyone else
   . work within all established 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)
   . only take photos or video of members of the school community with their consent
   . promptly report any evidence or reasonable suspicion of unauthorised access/use to the school leadership team
   . promptly report any accidental access to inappropriate to school staff

. 4.1.3 St Joseph's School Tranmere ICT Facilities or Personal ICT devices that access material on the school'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 member of the school community 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 School/CEO or any other network, or to deliberately degrade the performance of the School/CEO data network or communication devices supplied by the School or CEO

. 4.1.4 Members of the school community are responsible for the physical control and safe keeping of any digital electronic devices, mobile telecommunication devices, and other communication devices supplied to them by the School/CEO, 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 Members of the school community may use the school's ICT facilities for incidental personal use, provided such use is minimal and does not interfere with the performance of their duties, but are not permitted to use these ICT facilities to store or download large files (including music or movies) for personal use.

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

. 4.1.7 Members of the school community must promptly report to the principal any loss of, or unauthorised access to, any communication devices that contain work-related information or information that is otherwise confidential to the School/CEO.

. 4.1.8 Where a device that contains CESA data is lost or stolen School/CEO authorities reserve the right to erase all data on the device including any personal data.

. 4.1.9 Upon conclusion of their role within the School, Members of the school community must permanently remove from their Personal ICT Devices any work-related information, or information that is otherwise confidential to the School.

. 4.1.10 Members of the school community using CESA ICT Facilities (including Personal ICT devices that are used to access material on the school network) may be monitored by School and/or CEO personnel, and any evidence of use that contravenes this practice, or is otherwise inappropriate, may lead to disciplinary consequences.

. 4.1.11 In the case of an investigation into the conduct of a school community member, they must, if requested, provide their Personal ICT devices to the School/CEO 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.

. 4.1.12 When posting material in a Social Media forum (eg Facebook page, Twitter, blogs) members of the school community should be aware that such activity may be considered public, not private and therefore should be consistent with the Catholic ethos and the values espoused by Catholic Education South Australia

. 4.1.13 Staff 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 Members of the school community and students; or
  . divulge any confidential information, including students' personal information, through Social Media.

4.1.14 If someone else posts a comment or other material in a school community member's Social Media space, then if that comment or material:

  . is likely to cause serious damage to the relationship between the School/CEO and the school community member or
  . is likely to damage the interests of the School/CEO or
  . is incompatible with the school community member's duty to the School,

the school community member must (where possible) remove that comment or material as soon as it comes to their attention.

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 Members of the school community sign the Acceptable Use Agreement at the beginning of each school year (or when the school community member 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 Members of the school community in relation to the school's Acceptable Use Agreement and ICT Policy, and that new Members of the school community are made aware of the ICT 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 any known or suspected breaches of the school's ICT Policy and Acceptable Use Agreement that may constitute a criminal offence.

4.3 Responsibilities of school employees

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

. 4.3.1 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 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 promptly report to the Principal any known or suspected breaches of the school's ICT Policy that may constitute a criminal offence.

4.4 Consequences of Non-Compliance

In the event that a school community member is found to have breached the ICT 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 school community member's right to use the school's ICT Facilities.

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

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

5   Resources and Further Information

- Teacher, student and parent resources: E-safety website
  https://www.esafety.gov.au/
  http://www.cybersafekids.com.au/
  http://www.cybersafetysolutions.com.au/
- Social Networking Protocol for the Catholic Church
  http://mediablog.catholic.org.au/?p=335

6   Supporting Documents

- CESA Information and Communications Acceptable Use Baseline Standard Document (Sept 2014)
- CESA ICT Security Framework (Sept 2014)
- SACCS Information and Communications Security Policy (March 2015)
- CESA Privacy and Consent Form – (Nov 2013)
- St Joseph's School Tranmere Acceptable Use Agreement
- St Joseph's School Tranmere ICT Policy
- St Joseph's School Tranmere Procedures and Protocols for Digital Technologies
- St Joseph's School Tranmere Privacy Policy
- BYOD Guidelines

7   Glossary

- ICT device
- ICT platform
- School network and services

8   Revision Record

Document Title	St Joseph's School Tranmere ICT Policy
Document Type	Policy
Document Date	February 2016
Process Owner	Principal, St Joseph's School Tranmere
Contact	Clare Nocka ☎ 8431 2834 ✆ cnocka@stjotran.catholic.edu.au
Approval Authority	School Board, St Joseph's School Tranmere
Review Date	2017
Revision History	