

DIGITAL TECHNOLOGIES and SOCIAL MEDIA Staff and Student Policy

Policy Number: DTSM - SSP

Status: Ratified

Date Issued: 2012

Evaluation and Review: May 2016
Diocese of Lismore
MacKillop College Leadership Team.

Policy Contact Officer: Assistant Director – School Resources Services

Related Documentation:

Catholic Education in the Diocese of Lismore *Foundational Beliefs and Practices – The Essential Framework, 2007.*

The Vision and Mission of the Lismore Diocesan Catholic Education Board:

Media Policy

Privacy Policy

Child Protection Policy

Bullying & Harassment Policy

Grievance Policy

RATIONALE

“Information and Communications Technology in the workplace raises questions about the supervision of its use. This technology includes email and access to the Internet. The computers and internal network involved are controlled by the organisation and management has the responsibility for issuing clear instructions for their proper use. Without clear instructions, the proper use of email and web browsing may not be clear to many in the workplace.” Australian Privacy Commission 2005.

This Policy sets out information for all employees of the Trustees of the Roman Catholic Church of the Diocese of Lismore Catholic Schools Office, all teachers and ancillary staff in schools, parents, students, volunteers, visitors and contractors, (henceforth referred to as “technology users”) who may utilise digital technologies, this includes but is not limited to the provision of networks, services such as email, access to the Internet, data storage and the use of supplied or bring your own electronic devices and associated software which connect to the systems provided regarding the proper and permitted use of these digital technologies.

As part of the responsibilities of the Catholic Schools Office (CSO) towards ensuring safe and responsible electronic behaviours are occurring, technology users are made aware that their data, browsing activities and email content can be scrutinised, and random monitoring of sites visited may occur from time to time by authorised personnel. Users can be assured that the privacy of their communications and work-related activities will be respected. Users are expected to ensure that their professional and personal behaviour in relation to the use of digital technologies is consistent with this Policy.

This Policy is designed to inform all technology users of the proper and appropriate legislative, moral and ethical use of any data received, viewed, stored or transmitted using the Catholic Schools Office and individual Schools digital systems.

The adherence to this Policy is mandatory and any breaches of standards or behaviours that contravene the guidelines and practices detailed within the Policy will be subject to investigation which may lead to disciplinary procedures.

This Policy will be reviewed every two years or as required.

Scope

This Policy applies to all users as defined in the policy and sets out to maintain standards of operation and behaviour that protect the wellbeing of all technology users in the Diocese.

Definitions

- Trustees means The Trustees of the Roman Catholic Church Diocese of Lismore.
- CSO means the Catholic Schools Office of the Lismore Diocese.
- Electronic communication facilities refers to, but is not limited to: networks, PCs, laptops, iPods, iPads /tablets, audio devices, internet, intranet, mobile telephone devices, social web/media sites, email, e-portfolios, web 2.0 technologies, portable storage devices and Cloud technologies.

- Appropriately identified authority means person or persons responsible for administering compliance externally and internally. This list includes and is not limited to appropriate members of the CSO or recognised agencies.
- Technology users mean any individual:
 - i) supplied with, or having access to digital technologies which connect to or utilise the networks and services supplied by the Catholic Schools Office and individual schools.
 - ii) bringing their own digital device to the workplace, which may or may not connect to or utilise the networks and services supplied by the Catholic Schools Office and individual schools.
- Cyber-safe means material that is sent, stored or received via digital medium(s) that is in keeping with the intent of this document and causes no offence to any would be viewer or receiver of such material.
- ICT means Information Communication Technology.
- Flame-mail is the use of email to transmit offensive, insulting, harassing messages to other users or persons outside the workplace.
- Social Network sites are web based association sites of a professional or personal nature that facilitate networking opportunities. These include but are not limited to: Facebook, Twitter, LinkedIn, e-leader, chat rooms.

Introduction to Responsibilities

Technology users must be aware that the CSO and/or schools can be involved in litigation and relevant records relating to (persons) use and activities in relation to this Policy may be subpoenaed and must be kept.

Anything covered under this Policy is "discoverable" by way of court order or subpoena. These include matters affecting legal proceedings, personal affairs of any technology users even if communicated in confidence.

Data and email residing on or transmitted across a system is the property of the organization that owns the system. This has the support of recent decisions in the Courts. All electronic files are therefore the property of the CSO and/or school and email users should act on the basis that they can be and where necessary will be held accountable for every message issued from their machine, or authorized or issued on their behalf. This includes use of equipment provided to staff for use at home or away from the premises.

The responsibilities referenced in this document must be uppermost in the mind of all users involved in the teaching and supervision of students accessing digital technologies. Any person who is in doubt about whether the standards of the Policy apply or do not apply must consult with their designated supervisor.

Responsibilities

All members of the school community including religious, principals, assistant principals, teachers, school support staff, contractors, visitors, volunteers and CSO staff must:

- Ensure proper security and use of the digital technologies available to them and/or others in the schools environment.
- Ensure the use of the Catholic Schools Office (CSO) electronic communications system and devices requires respect for the law, for persons and for the Church, its mission and its values. It further requires integrity, diligence, economy and efficiency from the users of these facilities. All users of the CSO and/or school's internet and intranet must conduct their activities according to the principles and requirements laid out in this Policy.

1. Responsibility of the CSO

- Ensure that the Policy remains relevant.
- Ensure that all users of digital technology sign and agree to the Diocesan Policy and procedures.
- Ensure that breaches of the Policy are properly investigated and appropriate action is carried out and reported to the appropriate agencies.
- Ensure that all users have access to the Policy and that compliance with the Policy is reviewed and monitored through the school compliance audit process.

It is the responsibility of the Director to ensure this Policy is communicated to all employees of the Catholic Schools Office. To this end they will:

- Ensure appropriate procedures are developed from this Diocesan Policy and that all users sign and adhere to the Policy.
- Ensure all known reportable matters that may appear to contravene this Policy are communicated to the appropriate authority.
- Ensure that use of technology is in keeping with all matters relating to Child Protection legislation and protocols.
- Ensure the following:
 - i. Where the CSO chooses to provide links to other Internet sites from their Web pages an approval and review process should be incorporated to ensure that these links are, and remain, educationally appropriate. A warning indicating the transient nature of Internet material and sites should be associated with the links.
 - ii. That digital technology is provided for educational and administrative purposes and to conduct research and communicate with others. All users are required to act in a considerate and responsible manner and must not:
 - send or display offensive messages or pictures
 - use obscene language
 - bully, harass, insult or attack others
 - damage computers, computer systems or computer networks
 - violate copyright laws

- use another's password
- trespass in another's folders, work or files
- use the network for commercial purposes.

iii. That all users of technology understand the consequences of inappropriate use as detailed in this policy.

2. Responsibilities of Principals

It is the responsibility of the College Principal to ensure this Policy is communicated to all employees, parents, volunteers, visitors, contractors and students of the school. To this end they will:

- Ensure appropriate school policy and procedures are developed from this Diocesan Policy and that all users sign and adhere to the Policy.
- Ensure all known reportable matters that may appear to contravene this Policy are communicated to the appropriate authority.
- Work with CSO ICT staff to monitor and regulate the proper use of all digital technologies.
- Ensure that use of technology is in keeping with all matters relating to Child Protection legislation and protocols.
- Ensure the school technology policy include the following:
 - i. Where schools choose to provide links to other Internet sites from their Web pages an approval and review process should be incorporated to ensure that these links are, and remain, educationally appropriate. A warning indicating the transient nature of Internet material and sites should be associated with the links.
 - ii. That digital technology is provided for all for educational and administrative purposes and to conduct research and communicate with others. All users are required to act in a considerate and responsible manner and must not:
 - send or display offensive messages or pictures
 - use obscene language
 - bully, harass, insult or attack others
 - damage computers, computer systems or computer networks
 - violate copyright laws
 - use another's password
 - trespass in another's folders, work or files
 - use the network for commercial purposes.
 - iii. Ensure that all users of technology understand the consequences of inappropriate use as detailed in this policy.
 - iv. Appropriate reference to this policy as deemed necessary.
- Ensure staff educate students when using digital technologies and social media of any kind to:

- Respect themselves and others when publishing or communicating
- Create sensible, plain avatars, usernames and identities
- Set social networking security settings to private
- Keep personal information private
- Keep usernames and passwords secure and do not share them with anyone
- Report any inappropriate behaviour or content directed at them or others

3. Responsibility of All Users (other than students)

All users must abide by all of the following specific conduct requirements and those requirements set out in school specific policies in relation to their use of the network, Internet and Intranet, electronic data, email and use of electronic devices including mobile phones.

All users should not intentionally, in their use of CSO and/or school and/or personal digital technologies:

- Violate any State, Commonwealth or international law, or State or Commonwealth regulation, or fail to comply with CSO and/or school policies or procedures.
- Violate generally accepted social standards and ethical behaviour in digital communications. They should exercise good judgement, use appropriate language, and not send messages that are harassing, defamatory, threatening, abusive or obscene.
- Conduct any business or activity for commercial purposes or financial gain, including publishing material which contains any advertising or any solicitation of other network users or discussion group or list members to use goods or services.
- Download information or software from the Internet or Intranet which is not directly related to educational and administrative purposes without authorisation.
- View, store, upload, download, post, publish or circulate material inappropriate to the professional standards expected of a staff member working in a Catholic School, which may be: sexually related or pornographic; violent or hate related, racist, subversive, malicious, libellous or slanderous.
- Violate CSO and/or school or third party copyright, license agreements or other contracts.
- Seek to gain unauthorised access to any resources within or outside of the CSO and/or school.
- Disrupt or interfere with the intended use of the CSO and/or school's digital technologies including the Intranet and /or the global Internet and/or resources.
- Without authority destroy, alter, dismantle, disfigure, prevent rightful access to or otherwise interfere with the integrity of computer based information and/or information resources, including, but not limited to, uploading or creating computer viruses.

- Compromise or without authorisation invade the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources.
- Post to a discussion group or other public forum personal communications without the consent of anyone referenced in that discussion or posting.
- Conduct activity which may be defined as persistent, cyber-loafing, that is the use of the organisation's facilities and misuse of work time through accessing non-related work content and sites without authority.
- Attempt to read another person's electronic mail or other protected files.
- Reveal personal addresses or phone numbers of other users in any email communication without consent from the other person/s.
- Participate in Internet Relay Chat groups or sessions unless such session has been specifically set up to facilitate the communication between participants in a project or working group authorized by the CSO and/or school.
- Expose themselves, other users and entities to risk of legal action or adverse publicity by sending improper communications. Improper communications include "flame-mail".
- Publish/post or include in email messages, content or commentary on social network sites which might be deemed to defame an individual, a company or an organisation. This includes bullying, harassment or discriminatory behaviour based on age, gender, race, sexuality or disability.
- Make commentary or otherwise of others on social network and/or e-sites that could be considered offensive in any way or be in breach of any part of this Policy.
- Express opinions on social media or any other platform that are personal and not those of the CSO and /or School without a statement such as:
"I am an employee of a school / CSO and the view expressed is my own personal view and does not represent the views or policy of the CSO or School"
- Send anonymous messages, defined either as messages that do not contain details of the sender's name and affiliation, or messages sent through an anonymous email service.
- Use Facebook or other social media platforms for the purposes of learning and teaching in diocesan schools. Facebook and other social media are able to be used by schools for information dissemination and gathering provided alternative mechanisms are also available to provide this same service to parents and / or students.
- Have personal social networking sites and online profiles which are inconsistent with the professional standards expected of a staff member working in a Catholic School. School employees must ensure personal information is suitably protected using the available privacy settings. Teachers should not have Personal digital relationships with their students or invite students into personal social networking sites. All staff should use professional discretion if accepting ex-students or parents of current students as friends in social media accounts.

4. Responsibility of Student Users

All student technology users must abide by all specific conduct requirements set out in school specific policies in their use of digital technologies and social media including but not limited to the Internet and Intranet, email and other electronic devices including mobile phones.

5. Consequences of Inappropriate Behaviour

A user's conduct and behaviour in relation to the use of digital technologies including but not limited to email, internet, intranet and web browsing, social networking sites, mobile phones or other digital devices provided or used on site, may be deemed inappropriate if the contents of this Policy are found to have been breached.

If so, an investigation of the alleged breaches may take place. This investigation will be carried out by the appropriate authoritative figure or his/her delegate.

Failure to comply with this Policy may result in disciplinary action, up to and including dismissal or removal. Breaches of the Policy may also result in referral to law enforcement agencies.

Those who breach this or any other related Policies may have access to these services and equipment denied or removed and be subject to disciplinary action in accordance with the stated related policies

6. Privacy

All technology users need to be aware that from the beginning of 2013 the Catholic Schools Office will utilise service providers to provide certain services to the Catholic Schools Office, all schools, staff and students. In doing so it may provide your personal information to those service providers in connection with the provision of those services. The staff and student email service provider stores and processes emails outside Australia. Consequently your emails and email account details may be transferred, stored and processed in the United States or any other country utilised by Google to provide the Google Apps services. In using the office / school's email system you consent to this transfer, processing and storage of that information.

Catholic Schools Office personnel responsible for the email system may have the ability to access, monitor, use or disclose emails and associated administrative data for the purposes of administering the system and ensuring its proper use. In using the school's email system you consent to such access, use and disclosure.

Technology users are also advised that the use of cloud storage services should not be used to permanently store important or sensitive data in relation to the Catholic Schools Office, schools, parents, families or students as these files may be transferred, stored and processed in any country utilised by the service provider.

This Policy is endorsed and approved by the Executive of Catholic Schools Office Lismore on behalf of the Trustees of the Roman Catholic Church of the Diocese of Lismore.