



Catholic Schools Office Diocese of Lismore

DIGITAL TECHNOLOGIES STANDARD OPERATING PROCEDURE

SOP Number:	DTSOP03:04
Status:	Ratified
Date Issued:	April 2019
SOP Contact Officer:	Assistant Director – School Resource Services
Related Documentation:	<p>Catholic Education in the Diocese of Lismore Foundational Values for Catholic Identity and Mission</p> <p>Addressing Employee Performance and Disciplinary Matters Policy and Standard Operating Procedure</p> <p>Bullying & Harassment Policy and Standard Operating Procedure</p> <p>Child Protection Policy and Standard Operating Procedure</p> <p>CSO Retention and Disposal Standard Operating Procedure</p> <p>Employee Use of Social Media Standard Operating Procedure</p> <p>Privacy Policy and Standard Operating Procedure</p>

RATIONALE

The purpose of this Standard Operating Procedures is to provide guidelines for the acceptable use of digital technologies in the educational, administrative and personal contexts for employees of the Catholic Schools Office (CSO) and in parish schools. These guidelines reference an employee's use of devices, services and digital technologies in any context with students and parents and the maintenance of professional standards in an employee's own personal use of any digital technology.

This Standard Operating Procedure does not stand alone. It must be read and interpreted alongside other relevant CSO Policies and Standard Operating Procedures. This Standard Operating Procedure is related to the CSO Employee Use of Social Media Standard Operating Procedure and has been constructed to assist in protecting employees and to sustain a safe and supportive workplace and school environment that upholds human dignity.

Individual parish schools are to develop their own policy, procedures and guidelines to address digital technology use by students (including digital citizenship and acceptable use) being mindful and non-contradictory of these guidelines in doing so.

Technology users must be aware that the Catholic Schools Office and parish schools can be involved in litigation, and relevant records relating to use and activities in relation to this Standard Operating Procedure may be subpoenaed and must be kept.

Anything covered under this Standard Operating Procedure 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 organisation 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 and attachment issued from their device, or authorised 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 this Standard Operating Procedure apply or do not apply must consult with their designated supervisor.

SCOPE

This Standard Operating Procedure applies to all users as defined in the Standard Operating Procedure and sets out to maintain standards of use and behaviour that protect the wellbeing of all technology users in the Diocese

1. DEFINITIONS

- 1.1 **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.
- 1.2 **ARPANSA** means the Australian Radiation Protection and Nuclear Safety Agency. ARPANSA is the Australian Government's primary authority on radiation

protection and nuclear safety. ARPANSA regulates Commonwealth entities using radiation with the objective of protecting people and the environment from the harmful effect of radiation. ARPANSA undertakes research, provides services, and promotes national uniformity and the implementation of international best practice across all jurisdictions.

1.3 **CSO** means the Catholic Schools Office of the Lismore Diocese.

1.4 **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.

1.5 **Digital Citizenship** means the norms of appropriate and responsible behaviour with regard to technology use.

1.6 **Electronic communication facilities and platforms** means, but is not limited to:

- I. Local and wide area networks;
- II. Personal and school owned devices (e.g. PCs, laptops, iPods, iPads /tablets, printers, scanners and cameras;
- III. Audio and video devices e.g. Swivls;
- IV. Internet and intranet;
- V. Mobile phones;
- VI. Student owned devices;
- VII. Social web/media sites e.g. Facebook;
- VIII. Email and messaging services;
- IX. Forums, discussion boards and groups;
- X. Wikis (e.g. Wikipedia);
- XI. Vod and podcasts;
- XII. E-portfolios;
- XIII. Blogs and microblogs (e.g. Twitter)
- XIV. Web 2.0 technologies;
- XV. Physical and cloud based storage e.g.: USB, hard drive, Google Drive and iCloud;
- XVI. Video conferencing and web conferencing (VC) facilities;
- XVII. Cloud technologies, including the Google suite of products;
- XVIII. Software and software subscriptions;
- XIX. Apps and app purchasing; and
- XX. Platforms such as ClassDojo, Education Perfect, SeeSaw and FlipGrid.

1.7 **Flame-mail** means the use of email to transmit offensive, insulting, harassing messages to other users or persons outside the workplace.

1.8 **ICT** means Information Communication Technology.

- 1.9 **Non-Human Google Drive** means a Google Apps for Education Account owned by the parish school or CSO that facilitates the storage and sharing of data between members of that organisation.
- 1.10 **Social Network sites** means web based sites of a professional or personal nature that facilitate networking opportunities and online communication and interaction. These include but are not limited to: Facebook, Twitter, Instagram and LinkedIn.
- 1.11 **Technology users** means 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; or
 - 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.
- 1.12 **Trustees** means The Trustees of the Roman Catholic Church Diocese of Lismore.
- 1.13 **BYOD/BYODD/BYOT** means bring your own device, designated device or technology which may or may not connect to a CSO or parish school network.

2. RESPONSIBILITIES

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

- I. Ensure proper security and use of the digital technologies available to them and/or others in the Catholic Schools Office and parish school's environment; and
- II. Ensure the use of 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 systems. All users of the CSO and/or school's networks, internet and intranet must conduct their activities according to the principles and requirements set out in this Standard Operating Procedure.

3. RESPONSIBILITY OF THE CSO

3.1 It will be the responsibility of the Catholic Schools Office to:

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

3.2 It is the responsibility of the Director to ensure this Standard Operating Procedure is communicated to all employees of the CSO. To this end they will:

- I. Ensure appropriate procedures are developed from this Standard Operating Procedure and that all users sign and adhere to the Policy.

- II. Ensure all known reportable matters that may appear to contravene this Standard Operating Procedure are communicated to the appropriate authority.
- III. Ensure that use of technology is in keeping with all matters relating to Child Protection legislation and protocols.
- IV. Ensure the following:
 - a) 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;
 - b) 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, files or email; or
 - use the network for commercial purposes; and
 - c) That all users of technology understand the consequences of inappropriate use as detailed in this Standard Operating Procedure.

4. RESPONSIBILITIES OF PRINCIPALS

- 4.1 It is the responsibility of the school Principal to ensure this Standard Operating Procedure is communicated to all employees, parents, volunteers, visitors, contractors and students of the parish school. To this end they will:
 - I. Ensure appropriate school policies and procedures are developed from this Standard Operating Procedure and that all users sign and adhere to the Policy;
 - II. Ensure all known reportable matters that may appear to contravene this Standard Operating Procedure are communicated to the appropriate authority;
 - III. Work with CSO ICT staff to monitor and regulate the proper use of all digital technologies; and
 - IV. Ensure that use of technology is in keeping with all matters relating to Child Protection legislation and protocols.
- 4.2 It is the further responsibility of the Principal to ensure that school technology policy and procedure 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; and
- II. Supply information to employees about the appropriate storage of files related to the parish school, students and parents;
- III. 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, files or email; or
 - Use the network for commercial purposes.
- IV. Ensure that all users of technology understand the consequences of inappropriate use as detailed in this Standard operating Procedure;
- V. Make appropriate reference to this Standard Operating Procedure as deemed necessary; and
- VI. Ensure staff educate students when using digital technologies and social media of any kind to:
 - Respect themselves and others when publishing or communicating with the technology;
 - Create sensible, plain avatars, usernames and identities;
 - Set social networking security settings to private;
 - Keep personal information private;
 - Create strong passwords;
 - Keep usernames and passwords secure and do not share them with anyone; and
 - Report any inappropriate behaviour or content directed at them or others.

5. RESPONSIBILITY OF ALL USERS (OTHER THAN STUDENTS)

- 5.1 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, VC's, email, the Google suite of products and use of electronic devices including mobile phones.

- 5.2 All users should not keep permanently on their devices and/or personal cloud storage any administrative, confidential or sensitive files related to the employer, a student, class, cohort or parent. The CSO office R Drive, school G Drive or CSO/school Non-Human Account Google Drive is to be used as the storage repository for such files.
- 5.3 All users should not intentionally, in their use of CSO and/or school and/or personal digital technologies:
- I. Violate any State, Commonwealth or international law, or State or Commonwealth regulation, or fail to comply with CSO and/or school policies or procedures;
 - II. 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;
 - III. 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;
 - IV. Download information or software from the Internet or Intranet which is not directly related to educational and administrative purposes without authorisation;
 - V. 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;
 - VI. Violate CSO and/or school or third party copyright, license agreements or other contracts;
 - VII. Seek to gain unauthorised access to any resources within or outside of the CSO and/or school;
 - VIII. Disrupt or interfere with the intended use of the CSO and/or school's digital technologies including the Intranet, video conferencing facility and/or the global Internet and/or resources;
 - IX. 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;
 - X. Compromise or without authorisation invade the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources;
 - XI. Conduct activity which may be defined as persistent 'cyberloafing', that is the use of the organisation's facilities and misuse of work time through accessing non-work related work content and sites without authority;
 - XII. Attempt to read another person's electronic mail or other protected files;
 - XIII. Reveal personal addresses or phone numbers of other users in any email communication without consent from the other person/s;

- XIV. Participate in Video Conferencing, Skype or Google Hangout sessions unless such sessions have been specifically set up to facilitate the communication between participants in a project or working group authorized by the CSO and/or school;
- XV. Expose themselves, other users and entities to risk of legal action or adverse publicity by sending improper communications. Improper communications include 'flame-mail';
- XVI. 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;
- XVII. 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 Standard Operating Procedure;
- XVIII. 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";
- XIX. 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; or
- XX. Have personal social networking sites and online profiles which are inconsistent with the professional standards expected of an employee working in a Catholic School. Employees must ensure personal information is suitably protected using the available privacy settings.

5.4 Maintain a contemporary knowledge of digital citizenship.

5.5 Supervise and support students when using digital technologies in the classroom.

6. 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.

7. CONSEQUENCES OF INAPPROPRIATE BEHAVIOUR

- 7.1 A user's conduct and behaviour in relation to the use of digital technologies including but not limited to email, VC, intranet, internet 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 Standard Operating Procedure are found to have been breached.
- 7.2 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.
- 7.3 Failure to comply with this Standard Operating Procedure may result in disciplinary action, up to and including dismissal or removal. Breaches of the Standard Operating Procedure may also result in referral to law enforcement agencies.
- 7.4 Those who breach this or any other related Policies or Standard Operating Procedures may have access to these services and equipment denied or

removed and be subject to disciplinary action in accordance with the stated related policies and procedures.

8. PRIVACY

- 8.1 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 suite of services. In using the office / school's email system you consent to this transfer, processing and storage of that information.
- 8.2 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 email system, you consent to such access, use and disclosure.
- 8.3 Technology users also need to be aware that the use of personal or employer provided devices and cloud storage services should not be used to permanently store important or sensitive data in relation to the Catholic Schools Office, parish schools, parents, families or students. The CSO office R Drive, school G Drive or CSO/school Non-Human Account Google Drive is to be used as the storage repository for such files.

9. PASSWORD PROTECTION

- 9.1 Users must not disclose their password to anyone. User passwords must only be used to authenticate the user with information systems they have been granted access to.
- 9.2 Users must ensure that their password is protected from disclosure at all times.
- 9.3 Users must change their passwords in accordance with CSO policy.

10. EXPOSURE TO RADIOFREQUENCY (RF) ELECTROMAGNETIC ENERGY (EME) EMISSIONS FROM MOBILE PHONES AND OTHER WIRELESS DEVICES

For details and advice on RF EME emissions from mobile phones and other wireless devices refer to Appendix 1: ARPANSA's 'How to Reduce Exposure from Mobile Phones and Other Wireless Devices' Fact Sheet and Appendix 2: ARPANSA's 'Wi-Fi and Health' Fact Sheet.

VERSION HISTORY

Version	Approval Date	Authorised By	Notes
1	December 2012	Assistant Director – School Resources Services	Originally released
2	October 2015	Assistant Director – School Resources Services	Reviewed
3	April 2019	Assistant Director – School Resources Services	Reviewed, amended, reformatted



How to Reduce Exposure from Mobile Phones and Other Wireless Devices

There is no established scientific evidence that the use of mobile phones causes any health effects. However the possibility of a small risk cannot be ruled out. There are things one can do to substantially reduce exposure.

Overall, the evidence suggests that the radiofrequency (RF) electromagnetic energy (EME) emissions of mobile phone handsets are not harmful to the user.

However, it's impossible to be completely sure there isn't some risk. This is particularly true for children where there is little research evidence.

One way to exercise caution is to reduce unnecessary exposure from your handset and to encourage your children to do this. This can be done easily. Remember, it doesn't have to be for every phone call and in an emergency there are better things to worry about.

If you would like to reduce your exposure, here are some tips for doing so.

Mobile phones

You can reduce your exposure to RF EME from your mobile phone in three simple ways:

1. Distance

The most effective way to reduce the exposure is to increase the distance between your mobile phone and your head or body. You can do this by:

- using a wired ear-piece/microphone hands-free accessory
- using the phone on speaker mode
- texting rather than talking
- keeping the phone a distance from the body, as recommended in your phone's user manual
- even placing your thumb between the phone and your ear.

2. Time

If there are any harmful effects, then it's likely that the longer the exposure to RF EME the greater any risk may be.

You can reduce your exposure time by keeping voice calls short, especially when you are not using hands-free.

3. Power

Usually a phone in an area with good reception will transmit at much lower levels than in an area with poor reception like a lift or deep within a large building.

You can limit the amount of power your phone uses by:

- using your phone in good signal areas where possible (shown by lots of bars on the reception indicator)
- avoiding using your phone in poor signal areas such as lifts and moving vehicles. (Note: It is illegal to hold your phone to your ear while you are driving a motor vehicle.)

Cordless phones

Cordless phones generally have lower maximum power levels than mobile phones but don't all have the same automatic reduction in power that mobile phones have. Also the bases of many cordless phones are continually transmitting low-level signals.

You can reduce your exposure to RF EME from cordless phones by:

- using speaker mode
- limiting the length of the call
- keeping your distance from the cordless phone base unit
- using a wired land-line phone.

Due to the lack of scientific evidence on mobile and cordless phone use by children, ARPANSA recommends that parents encourage their children to limit their exposure.

Other wireless devices

Many other household wireless devices use RF EME to communicate, including:

- wireless computer networks
- audio-visual transmitters
- wireless security cameras, and
- baby monitors.

In typical use RF EME exposures from these devices are usually well below the limits of the Australian standard. However, if you use them with their antennas very close to the body, you can be exposed to levels closer to the limits of the standard.

You can reduce your exposure from these devices by:

- keeping them at a distance, for example placing the wireless router away from where people spend time
- reducing the amount of time you use them.

Protective devices

Be aware that some so-called protective devices may not reduce RF EME.

Mobile phone devices

These products are attached to the handset and take the form of shielded cases, earpiece pads/shields, antenna clips/caps and absorbing buttons.

- A cover or device that separates the phone from the head will reduce exposure to some extent but may interfere with the phone's ability to automatically reduce its power.
- Tests have shown that many of these devices can reduce your exposure when the phone is set to transmit at maximum power. However, because phones have automatic power control, these shields make the phone work harder, transmitting more power, increasing heat and reducing battery life. The incoming signal to the phone will also be reduced so the phone may not work in poor signal areas.

'Neutralising' products

Some products that attach to the phone are advertised as neutralising any harmful effects. Their claims are not consistent with current scientific knowledge and it is difficult, if not impossible, to verify any benefits.

Although sellers of some of these devices have reported biological tests to support health claims, there is no reliable evidence that such devices provide any health benefits other than by perhaps reducing people's anxiety or by a placebo effect.

ARPANSA does not recommend the use of any protective devices other than approved hands-free accessories that let you keep the phone away from the head during use.

Useful links

ARPANSA fact sheet on RF EME

www.arpansa.gov.au/RadiationProtection/basics/rf.cfm

ARPANSA fact sheet on mobile phones and health effects

www.arpansa.gov.au/mobilephones

WHO fact sheet on mobile phones

www.who.int/mediacentre/factsheets/fs193/en

The ARPANSA RF Standard

www.arpansa.gov.au/Publications/codes/rps3.cfm



Fact Sheet

Wi-Fi and Health

There is no established scientific evidence showing that the low exposure to radiofrequency electromagnetic energy from Wi-Fi adversely affects the health of children or the general population.

What is Wi-Fi

The use of Wi-Fi has increased rapidly in recent years. Through the use of this technology, electronic devices are connected to a computer network wirelessly using radio waves, or radiofrequency (RF) electromagnetic energy (EME), thereby eliminating or reducing the need for network cables. A common example is a laptop connected to the internet using a Wi-Fi modem at home. Wi-Fi access points can also be found in schools and many public areas. People in a Wi-Fi enabled environment will be exposed to low level RF EME from time to time when using the network on computers and also from the access points. There is some public concern about potential health effects associated with RF EME emissions from Wi-Fi in homes, schools and other places.

Is Wi-Fi regulated in Australia?

The RF EME emissions from Wi-Fi and other wireless devices used for communication are regulated by the Australian Communications and Media Authority (ACMA). ACMA's regulatory arrangements require wireless devices to comply with the exposure limits in the ARPANSA RF Standard. The ARPANSA Standard is designed to protect people of all ages and health status against all known adverse health effects from exposure to RF EME. The ARPANSA Standard is based on scientific research that shows the levels at which



harmful effects occur and it sets limits, based on international guidelines, well below these harmful levels.

Does Wi-Fi cause any health effects?

It is the assessment of ARPANSA and other national and international health authorities, including the World Health Organization (WHO), that there are no established adverse health effects below current exposure limits.

Wi-Fi devices and access points are low powered, typically 0.1 watt (100 milliwatts). Measurement surveys have shown that exposure to RF EME from Wi-Fi in schools is expected to be much lower than the limit for public exposure specified in the ARPANSA Standard.

Can I reduce my exposure to Wi-Fi?

There are no established adverse health effects from the Wi-Fi RF exposure. However, if you wish to reduce your exposure you can do so by:

- increasing the distance to Wi-Fi equipment
- reducing the amount of time you use Wi-Fi equipment.

What does ARPANSA advise?

On the basis of current scientific information, ARPANSA sees no reason why Wi-Fi should not continue to be used in schools and in other places. However, ARPANSA recognises that exposure to RF EME from Wi-Fi and other wireless devices can be of concern to some parents. ARPANSA will continue to review the research into potential health effects of RF EME emissions from Wi-Fi and other devices in order to provide accurate and up-to-date advice.

Useful Links

ARPANSA fact sheet on RF EME

www.arpansa.gov.au/RadiationProtection/basics/rf.cfm

The ARPANSA RF Standard

www.arpansa.gov.au/RadiationProtection/Factsheets/is_rfStandard.cfm

ARPANSA provides general advice on reducing exposure from wireless devices

www.arpansa.gov.au/RadiationProtection/Factsheets/is_Wireless.cfm

WHO fact sheet on wireless technologies

www.who.int/peh-emf/publications/facts/fs304/en/

Wi-Fi in schools measurement survey in the UK

<http://webarchive.nationalarchives.gov.uk/20140714084352/http://www.hpa.org.uk/Topics/Radiation/UnderstandingRadiation/UnderstandingRadiationTopics/ElectromagneticFields/RadioWaves/WiFi/WiFiprojectreportonresultsSeptember2011/>

More information is available on the ARPANSA website www.arpansa.gov.au.