Catholic Schools Office
DIOCESE OF MAITLAND-NEWCASTLE

WORKPLACE INTERNET, EMAIL AND NETWORK USAGE POLICY

November 2016

DOCUMENT SUMMARY	
Responsible Officer	Assistant Directors
Effective Date	November 2016
Superseded Docs	Workplace Internet, Email & Network Usage (Revised 2013)
Review Date	November 2017
School Actions	Schools are to ensure their practices are consistent with this policy. A local policy is not required.
Associated Docs	Privacy Policy (2016)

NATURE AND P URPOSE OF THE CATHOLIC SCHOOL

Inspired by the message and example of Jesus Christ, Catholic schools live out a distinctive educational vision. Supported by the Catholic community of which they are a vital part, they invite students and their families into a faith-filled educational experience.

As a key ministry of parishes and the diocese, Catholic schools encourage and support parents in their responsibility for the faith formation of their children. This formation is supported by prayer and opportunities to participate in the life, mission and liturgy of the broader Catholic community.

Our schools commit to:

- nurturing each individual's growth in faith and unique potential
- offering outstanding educational experiences founded on Catholic values
- fostering partnership between parents and staff in the education of their children
- creating communities of respect for each other, the wider society and the earth
- encouraging active engagement in social justice issues, the service of others and the promotion of peace.

Catholic schools are part of a long tradition of Catholic education provided by religious and lay teachers in Australia and this diocese for over 180 years. They fulfil parents' rights to choose the schooling for their children which reflects their own values, beliefs and hopes.

Workplace Internet, Email and Network Usage Policy

CONTENTS

1. RATIONALE

Internet and digital technology offer an opportunity for teachers to enhance students' learning by providing unprecedented access to information. The Catholic Schools Office provides email facilities and Internet access to support the educational mission of the schools. As well, the schools network provides assistance with the administration of all schools in the Maitland-Newcastle Diocese, to enhance the curriculum and learning opportunities for students and staff and to provide productivity benefits to school and CSO staff.

The rapid growth of mobile phone communication, social media and digital storage devices coupled with advances in the development of emerging technologies warrants the ongoing review of safety policies and procedures. This is required to maintain a safe learning and working environment for students and staff in Catholic schools and offices within the Diocese. The Catholic Schools Office has a responsibility to staff and students for ensuring clear instructions for proper use to protect both the network and its moral integrity.

While embracing these opportunities we are reminded of the words of Pope John Paul 11;

> *The internet offers extensive knowledge, but it does not teach values; and when values are disregarded, our very humanity is demeaned and man easily loses sight of his transcendent dignity. Despite its enormous potential for good, some of the degrading and damaging ways in which the Internet can be used are already obvious to all, and public authorities surly have a responsibility to guarantee that this marvellous instrument serves the common good and does not become a source of harm.* (Pope John Paul 11, 2002)

2. AIMS

This policy aims to:

2.1 Provide clear, unambiguous information to all employees concerning the appropriate use of the Catholic Schools Office computer facilities and external networks.

2.2 Provide clear, unambiguous information to all employees about the use of ICT equipment / devices connected to the school's network or brought onto the school property and/or a school activity.

2.3 Assist in the development of good and appropriate practices with regard to the use of email, social media and the internet in the workplace, for employees in the Diocese of Maitland-Newcastle.

2.4 Support the development of appropriate practice with regard to the use of email, social media and the internet by students.

2.5 Provide parents with clear guidelines to support appropriate participation in their school's social media Facebook page.

3. IMPLEMENTATION

3.1 Staff are to utilise CSO and school computers, networks and Internet services for office and school-related purposes and performance of job duties. Incidental personal use of CSO and school computers is permitted, as long as such use does not interfere with the employee's job duties and performance, with system operations or other system users

3.2 All users need to be aware that their browsing activities and email, social media content can be scrutinised.

3.3 System administrators are able to access user data and log network use as part of their role. In reviewing and monitoring user accounts and information, the CSO system administrators (including the Director of Schools, Head of Financial Services and nominated ICT personnel) will respect the

privacy of individuals. These people must not divulge or disclose such information to others unless required by the Director of Schools, Head of Financial Services or State or Commonwealth Law. (ref. National Privacy Principles 2001).

3.4 All staff need to be aware of the issues related to Cybersafety and they need to ensure they follow and encourage positive online behaviour. Staff must ensure that their online behaviour in relation to students is at all times professional and that they are aware of their duty of care to students. This includes their use of online social networking sites.

3.5 Ongoing professional development enabling staff to maintain an understanding of, this rapidly changing environment is required regularly. Selected and age appropriate resources are available on MNworks or the CSO webpage.- www.mn.catholic.edu.au

3.6 IT IS THE RESPONSIBILITY OF ALL STAFF TO:

3.6.1 Obtain authorisation prior to using CSO computer facilities and external networks, including the internet, through the use of user identification and passwords.

3.6.2 Ensure that the contents stored on any ICT equipment / device they join to the school network or bring to the school property and/or school activity is appropriate and acceptable, as defined in the Workplace Internet, Email and Network Usage - Code of Practice School Staff (Support Document 1). This includes but is not limited to mobile phones, computers, storage devices and iPods.

3.6.3 Report any inappropriate behaviour or material related to the use of internet or communication services to their supervisor.

3.6.4 Ensure they have read, signed and understand all elements of this Workplace Email, Internet and Network Usage Policy.

3.6.5 Be aware that any breach of this policy may result in disciplinary action. This may include termination of employment.

3.7 IT IS THE RESPONSIBILITY OF PRINCIPALS OR THEIR DELEGATE TO:

3.7.1 Implement the Workplace Internet, Email and Network Usage - Staff Code of Practice (Support Document 1) and ensure all staff members have returned a signed copy of the Staff Code of Practice prior to being granted access to the school's network.

3.7.2 Follow the guidelines as outlined in the Setting up Social Media Pages for Schools Procedure document before any school social media pages are activated.

3.7.3 Develop and implement a Cybersafety User Agreement for students (refer to samples in Support Document 3 / 4).

3.7.4 Ensure that student access will be appropriately supervised as determined by the school.

3.7.5 Conduct a review in accordance with the Staff Incident Report procedure (Support Document 5 / 6) should a staff member breach of the Workplace Internet and Network Usage Policy occur.

3.7.6 Conduct a review in accordance with the Student Incident Report procedure (Support Document 7 / 8) should a student breach of the Cybersafety User Agreement occur.

3.7.7 Advise staff NOT to open content suspected of being child pornography.

3.8 IT IS THE RESPONSIBILITY OF THE CSO ASSISTANT DIRECTORS OR DELEGATE TO:

3.8.1 Ensure that the authorised use of computer facilities and external networks, including the internet, is consistent with principles, regulations and laws relating to the privacy and safety of school students, staff and CSO staff.

3.8.2 Discuss with Principals their school needs in relation to social media before official pages are activated.

3.8.3 Participate fully when the relevant Assistant Director is consulted as part of the incident procedure (Support Document 5 / 6 or 7 / 8) following a reported breach in a school of the Workplace Ensure Internet and Network Usage Policy. This may involve analysis by CSO ICT staff or other relevant experts.

3.8.1 Ensure that the authorised use of computer facilities and external networks, including the internet, is consistent with principles, regulations and laws relating to the privacy and safety of school students, staff and CSO staff.

3.8.2 Discuss with Principals their school needs in relation to social media before official pages are activated.

3.8.3 Participate fully when the relevant Assistant Director is consulted as part of the incident procedure (Support Document 5 / 6 or 7 / 8) following a reported breach in a school of the Workplace Ensure Internet and Network Usage Policy. This may involve analysis by CSO ICT staff or other relevant experts.

3.8.4 Conduct an investigation as part of the incident procedure (Support Document 9 / 10) following a reported breach at the CSO of the Workplace Ensure Internet and Network Usage Policy. This may involve analysis by CSO ICT staff or other relevant experts.

3.8.5 Contact the Police and Zimmerman Services in the suspected case of staff accessing child pornography. The Crimes Amendment Act (Child Pornography) NSW Schedule 1, lists possession of child pornography as an offence.

3.9 PROCEDURES

3.9.1 The Director and Heads of Service need to ensure that all CSO staff have returned a signed copy of the Staff Code of Practice (Support Document 2) to them prior to being granted access to the CSO's network.

3.9.2 Permanent staff and those staff employed for more than 20 consecutive days will be issued with a unique user name and password. Casual staff (employed for less than 20 consecutive days) may be issued (at the discretion of the Principal / Head of Service or his/her appointee) with a casual network account with a unique password.

3.9.3 Staff are solely accountable for all actions performed under their username and password and will be required to sign a Workplace Internet, Email and Network Usage Code of Practice (Support Documents 1 or 2) before using the network account and therefore must not divulge their password to anyone.

3.9.4 The Catholic Schools Office ICT Manager in collaboration with CSO Assistant Directors will be responsible for the oversight of this policy. Other CSO personnel including the Assistant Directors and Teaching and Learning Services will provide guidance and support to schools in relation to this policy.

4. BUDGET

The Catholic Schools Office will devote a proportion of its budget to the provision of funds for professional development to support staff in relation to this policy. It is recommended that schools budget for additional costs, where necessary, for the ongoing implementation of this Policy.

5. EVALUATION

This policy will be reviewed every three years by the Assistant Directors in consultation with relevant staff.

6. GLOSSARY

For the purposes of this Policy, the following definitions apply:

Computer Facilities and External Networks – includes the school's and or CSO's computers and all hardware, software, networks, internet and email.

ICT equipment/devices – including but not limited to, computers (such as desktops, laptops, PDAs, storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players) cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players) and any other, similar, technologies as they come into use.

Employees - people employed in teaching and non-teaching positions in schools and the Catholic Schools Office, Diocese of Maitland-Newcastle

CSO – Catholic Schools Office

Zimmerman House – Diocesan child protection and professional conduct unit

Computer Facilities and External Networks – includes computers, local area networks, connections to external electronic networks, and subscriptions to external network services.

Internet – refers to the global network of multi-platform smaller computer networks which allows the user to access information, communicate and collaborate electronically.

Incidental personal use – is defined as use by an individual employee for occasional personal communications.

Social Media – Social media is defined as any form of online publication or presence that allows interactive communication, including, but not limited to, social networks, blogs, internet websites, internet forums, and wikis. Examples of social media include, but are not limited to, Facebook, Twitter, YouTube, Google+, and Flickr.2

Unacceptable use – refers to but not limited to the following
To send, forward, attach, upload, transmit, download, link to or store any images, content, links or material that:

- Is, or may be construed to be, defamatory, harassing, threatening, vilifying, racist, sexist, sexually explicit, pornographic, or otherwise offensive.
- Is, or may be construed to be, insulting, vulgar, rude, disruptive, derogatory, harmful or immoral.
- Harasses or promotes hatred or discrimination based on any unlawful grounds against any person.
- Contains any virus, worm, Trojan or other harmful or destructive code.
- Relates to the manufacture, use, sale or purchase of illegal drugs or dangerous materials or to any other illegal activity.

- Injures the reputation of the Catholic Schools Office and/or school or cause embarrassment to the Catholic Schools Office and/or school.
- Is span or mass/chain mail.
- Communicates information concerning any password, identifying code, personal identification code or other confidential information.
- Infringes the copyright or other intellectual property rights of another person.
- Involves gaming, waging or betting.
- Is personal business activity for financial gain or commercial purposes.
- Is defined as illegal activities under the Australian Commonwealth Government Telecommunications Act 1997 or Crimes Act, NSW, 1900 Section 578C, Crimes Amendment Act (Child Pornography) NSW Schedule 1.

7. SUPPORT DOCUMENT CONTENTS

SEPARATE DOCUMENT

1. Workplace Internet, Email and Network Usage – Code of Practice – School Staff
2. Workplace Internet, Email and Network Usage – CSO and other non-School Workplace staff
3. Cybersafety User Agreement for Primary Schools
4. Cybersafety User Agreements for Secondary Students
5. School Staff Incident Report Flowchart
6. School Staff Incident Report
7. Student Incident Report Flowchart
8. Student Incident Report
9. CSO Staff Incident Report Flowchart
10. CSO Staff Incident Report
11. Parent Declaration for Social Media Involvement