WORKPLACE INTERNET, EMAIL AND NETWORK USAGE POLICY FEBRUARY 2017

1. PURPOSE

This policy aims to:

i. Provide clear, unambiguous information to the staff in regard to the appropriate use of the school's computer facilities and network.
ii. Provide clear and unambiguous information to the staff about the use of ICT equipment / devices connected to the school's network or brought onto the school property.
iii. Assist in the development of 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.
iv. Support the development of appropriate practice with regard to the use by students of email, social media and the internet.

2. POLICY STATEMENT

Internet and digital technology offer an opportunity for teachers to enhance students' learning by providing unprecedented access to information. The school provides email facilities and internet access to enhance the curriculum and learning opportunities for our students. The rapid growth of mobile phone communication, social media and digital storage devices, coupled with advances in the development of emerging technologies, warrant the ongoing review of safety policies and procedures. The school has a responsibility to staff and students for providing clear instructions for proper use to protect both the network and its moral integrity.

3. SCOPE

This policy applies to all staff members who use the school's computer facilities and network.

4. GUIDING PRINCIPLES

We are reminded of the words of Pope John Paul II: "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 surely have a responsibility to guarantee that this marvellous instrument serves the common good and does not become a source of harm." (Pope John Paul II, 2002).

5. RESPONSIBILITIES

i. Staff are to utilise school computers, networks and internet services for school-related purposes and performance of job duties. Incidental personal use of school computers is permitted, as long as such use does not interfere with the employee's job duties and performance, with system operations, or with other system users.
ii. All users need to be aware that their browsing activities and email, social media content can be scrutinised.
iii. All staff need to be aware of the issues related to Cybersafety and they must ensure that 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.
iv. 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 and the CSO webpage.- www.mn.catholic.edu.au.
v. It is the responsibility of all staff to:
    a. Obtain authorisation prior to using CSO computer facilities and external networks, including the internet, through the use of user identification and passwords.

b. Ensure that the contents stored on any ICT equipment / device they join to the school network or bring to the school property is appropriate and acceptable, as defined in the CSO's 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.
c. Report to the principal any inappropriate behaviour or material related to the use of internet or communication services.
d. Ensure that they have read, signed and understand all elements of this Workplace Internet, Email and Network Usage Policy.
e. Be aware that any breach of this policy may result in disciplinary action. This may include termination of employment.

vi. It is the responsibility of the principal or his/her delegate to:
a. Implement the Workplace Internet, Email and Network Usage - Staff Code of Practice (Support Document 1) and ensure that all staff members have returned a signed copy of the Staff Code of Practice prior to being granted access to the school's network.
b. Follow the guidelines as outlined in the Setting up Social Media Pages for Schools Procedure document before any school social media pages are activated.
c. Develop and implement a Cybersafety User Agreement for students. (Refer to samples in Support Document 3 / 4).
d. Ensure that student access will be appropriately supervised as determined by the school.
e. Conduct a review in accordance with the Staff Incident Report procedure (Support Document 5 / 6) should a staff member breach the Workplace Internet, Email and Network Usage Policy.
f. Conduct a review in accordance with the Student Incident Report procedure (Support Document 7 / 8) should a student breach the Cybersafety User Agreement.
g. Advise staff not to open content suspected of being child pornography.

6. BUDGET

The school will devote a proportion of its budget to the provision of funds for professional development to support the staff in relation to this policy.

7. NEXT REVIEW DATE

This policy will be reviewed in 2020 in consultation with relevant staff.

8. DEFINITIONS

i. Computer facilities and external networks: Includes the school's computers and all hardware, software, networks, internet and email.
ii. ICT equipment / devices: Includes, but is 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.
iii. Employees: People employed in teaching and non-teaching positions in schools and the Catholic Schools Office, Diocese of Maitland-Newcastle
iv. CSO: Catholic Schools Office.
v. Zimmerman House: Diocesan child protection and professional conduct unit.
vi. Internet: Refers to the global network of multi-platform smaller computer networks which allows the user to access information, communicate and collaborate electronically.
vii. Incidental personal use: Use by an individual employee for occasional personal communications.
viii. Social media: 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.
ix. Unacceptable use: Refers to the sending, forwarding, attaching, uploading, transmitting, downloading, linking to storing of any images, content, links or material that:

a. Is, or may be construed to be, defamatory, harassing, threatening, vilifying, racist, sexist, sexually explicit, pornographic, or otherwise offensive.
b. Is, or may be construed to be, insulting, vulgar, rude, disruptive, derogatory, harmful or immoral.
c. Harasses or promotes hatred or discrimination based on any unlawful grounds against any person.
d. Contains any virus, worm, Trojan or other harmful or destructive code.
e. Relates to the manufacture, use, sale or purchase of illegal drugs or dangerous materials or to any other illegal activity.
f. Injures the reputation of the Catholic Schools Office and/or school or cause embarrassment to the Catholic Schools Office and/or school.
g. Is span or mass/chain mail.
h. Communicates information concerning any password, identifying code, personal identification code or other confidential information.
i. Infringes the copyright or other intellectual property rights of another person.
j. Involves gaming, waging or betting.
k. Is personal business activity for financial gain or commercial purposes.
l. 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.

9. LEGISLATIVE / PROFESSIONAL GUIDELINES

i. Workplace Internet, Email and Network Usage – Code of Practice – School Staff
ii. Workplace Internet, Email and Network Usage – CSO and other non-School Workplace staff 3.
iii. Cybersafety User Agreement for Primary Schools
iv. School Staff Incident Report Flowchart
v. School Staff Incident Report
vi. Student Incident Report Flowchart
vii. Student Incident Report