Related Policies

Copyright

Media Usage

Offshore Data Hosting

Privacy

Web Publishing

Purpose

Computer facilities and external networks are made available as resources for use by students in Catholic Schools in the Archdiocese of Canberra and Goulburn. The purpose of this Policy is to highlight the significant educational value of Information and Communications Technologies (ICT) in a safe and supportive environment, whilst decreasing the risk of exposure to inappropriate and offensive material or behaviours. School Principals and leaders in education have a responsibility to ensure that procedures are in place for the acceptable use by students of computer technology, email, Internet services, social media and other technology based systems within Catholic Schools.

Policy

It is the policy of the Catholic Education Office (CEO) that School based procedures for the use of computer facilities and external networks are based on the following principles:

- the use of technology must reflect the teaching and educational goals of the Catholic School and System. Access to and content of technology use must always be referenced to curriculum and developmental educational needs of the students.
- all employees' duty of care for students extends to the procedures and practices of computer usage and access of students to ICT .
- technology based information created, produced, communicated, stored or accessed on school ICT are subject to monitoring by the school or CEO.
- access to ICT by students is a privilege and with this comes the responsibility of appropriate usage, which may be revoked for not following the school's acceptable use standards. Other consequences may be considered by the school due to the severity of the breach of the Policy.
- student use of ICT must not be contrary to relevant Territory, State or Commonwealth laws. This includes, but is not limited to, laws regarding the possession or transmission of pornography including child pornography, anti-bullying legislation, harassment, anti-discrimination legislation, privacy laws, and laws concerning the improper use of technology with criminal intent.
- Parents/guardians must be regularly informed of the Policy and be encouraged to assist in facilitating its implementation.
- students must read and sign (if age appropriate) the Acceptable Use Agreement, which must be co-signed by a parent/guardian. Examples of these documents are included at the end of this Policy. Generally, students from Pre-Kindergarten through Year 2 will be considered too young to sign the Acceptable Use Agreement of their own accord. A parent/guardian will sign for these students and document that they have read and explained the agreement to their child.

Definitions

Acceptable use includes those lawful uses that are related to the core business of the CEO and its system of schools and includes incidental personal use of CEO and school computers and devices, as long as such use does not interfere with system operations or other system users.

Computer facilities and external networks includes computers and other ICT user devices, local area networks, connections to external electronic networks and subscriptions to external network services.

Devices include but are not limited to desktops, laptops, tablets, mp3 players, iPods, USB storage devices and mobile phones, regardless of who they belong to, that are brought onto the CEO or school property or to school activities, or that are connected to the school's network or facilities.

Inappropriate material means material which is inappropriate or harmful for children and includes:

- Child abuse images: depictions of children being sexually abused or posing inappropriately.
- Pornography: depictions of adults engaged in sexual activity.
- Nudity: depictions of detailed nudity.
- Violence: depictions of violence that is particularly strong in impact.
- Illegal activity: content which promotes or instructs in criminal activity.
- Terrorist related material: content that advocates terrorist activities.
- Other material that may require an adult perspective.

Incidental personal use is defined as use by an individual student for occasional personal communications provided that such use is lawful and complies with this Policy.

Information and Communication Technology (ICT) means all computer hardware, software, systems and network infrastructure.

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

Personal electronic device means a piece of electronic equipment, such as a laptop computer or a mobile phone, that is small and easy to carry and that belongs to an individual rather than being CEO property.

Social media are any form of online publication or presence that allows interactive communication. Social media sites include but are not limited to:

- micro-blogging sites, eg Twitter
- social networking sites, eg Facebook, MySpace
- video and photo sharing sites, eg YouTube, Flickr
- weblogs, including corporate or personal blogs
- forums and discussion boards, eg Yahoo! Groups or Google Groups
- wikis, eg Wikispaces, Wikipedia
- multiplayer gaming sites eg World of Warcraft
- virtual world sites eg Second Life

Software means electronic computer instructions or data (whether licensed, shareware, freeware, evaluation or otherwise) and includes system software, application software or data files.

Procedures

1. The CEO will:

1.1 monitor the use of computer technology, email, Internet services, social media and other technology based systems with the aim of ensuring that such use by students in the CEO's systemic schools relates to the educational goals of the schools and is consistent with principles, regulations and laws relating to the privacy and safety of school students.

1.2 provide appropriate software, either onsite or by the service provider, to seek to allow students to have access only to appropriate online sites.

1.3 regularly monitor and review the use of its computer facilities and external networks.

1.4 take such lawful action as it deems necessary to protect the security of its assets, facilities and networks.

1.5 take such lawful action as it deems necessary to fulfil its duty of care to students including the blocking of Internet sites, restricting a user's access and the confiscation of devices.

2. School Principals will:

2.1 implement the Policy.

2.2 ensure that an appropriate Acceptable Use Agreement (see Appendix A for example) is signed annually by parents/guardians and students (Year 3 and up) and placed on record in the school before a student is allowed to access the school's computer facilities and network. The Agreement should include a clear statement to parents/guardians about any systems available to students, such as Google email, where data is stored offshore.

2.3 provide appropriate instruction to enable students to understand and agree to comply with the requirements of the Acceptable Use Agreement.

2.4 provide education programs for students that focus on ethical and acceptable uses of the Internet as well as appropriate online etiquette.

2.5 provide education programs for students which develop protective behaviours when accessing online environments.

2.6 endeavour to provide reasonable supervision of student compliance with the Acceptable Use Agreement and to investigate alleged breaches of the Acceptable Use Agreement by students and to implement appropriate consequences.

2.7 highlight to students the possible dangers of communicating personal information on the Internet, especially in but not limited to social media sites.

2.8 inform students that they may not be able to delete items that they store on social media sites.

2.9 inform students of the legal, social and civic implications of their online behaviour.

2.9 obtain from a parent/guardian, annual written permission as part of the Acceptable Use Agreement for students to publish or transmit student work which may or may not include identifying student information.

2.10 work with the CEO to monitor the use of the school's computer facilities and external networks and inform users that this monitoring occurs (see point 6 below).

3. All students will:

3.1 obtain authorisation to use CEO computer facilities and external networks, including the Internet, through the use of their own personal passwords and user identification.

3.2 only download or install software in accordance with the instructions provided by CEO IC&LT Services and/or the school's authorised personnel.

3.3 only use their school's computer facilities and external networks for acceptable use and in accordance with this Policy, other relevant policies and the Acceptable Use Agreement.

3.4 take full responsibility for the effect that their actions and words may have on others.

3.5 if unsure as to the appropriateness of their online behaviour seek guidance from a teacher or a parent/guardian.

3.6 immediately report to a teacher or parent/guardian upon becoming aware of:

- any breach of security, confidentiality or privacy.
- receipt or accidental download of inappropriate or offensive material.
- receipt or presence of any virus .
- any breach or alleged breach of the Acceptable Use Agreement.

3.7 read and sign the Acceptable Use Agreement if they are in Year 3 or above before using the school's computer facilities and external networks.

4. A parent/guardian will:

4.1 read and sign the Acceptable Use Agreement and the Use of Personal Devices Agreement (if applicable) before their child is allowed to use the school's computer facilities and external networks.

5. Use of Personal Electronic Devices

5.1 Each school will determine whether personal electronic devices will be allowed at school and, if so, which devices will be included. However, all personal electronic devices brought to the School will be governed by this Policy. Principals need to take into account the range of devices that will be supported on the CEO network as listed in the Service Level Agreement. Parents/Guardians of students wishing to authenticate a personally owned computer or other approved device to the school's network must sign a Personal Electronic Device Use Agreement (see Attachment B) that outlines the level and type of support available and the end user's responsibility in managing the device. Students in Years 3 or above should also read and sign this agreement.

5.2 Devices owned by students may be searched and /or confiscated if the Principal believes, on reasonable grounds, that there is a threat to a person or system security or the device has been used or involved with unlawful conduct or a serious breach of the Acceptable Use Agreement.

5.3 Whilst using personal electronic devices at school, students MUST access the Internet through the school wireless network.

5.4 Maintenance of personal electronic devices is NOT a school responsibility.

5.5 It is the responsibility of students to purchase and upgrade software for their personal electronic device and to charge batteries.

5.6 The school will not be liable for loss or damage to personal electronic devices, beyond circumstances covered in the school's Behaviour Management Policy. Students are NOT to lend their personal electronic devices to others whilst at school. Arrangements to securely store devices must be made when those devices are not in use. Schools will develop their own storage policies.

5.7 Whilst at school students must not use their personal devices to take photographs or record video or sound without the permission of a teacher and the permission of all people being photographed or recorded.

6. Monitoring

6.1 From time to time the content and usage of student email and other electronic communications may be examined by the School Principal, the CEO or a third party on the CEO's behalf

6.2 All student messages and files on the CEO's system will be treated as education related and may be monitored. Accordingly students should not expect that any message or file transmitted or stored on their school's computer facilities and external networks will be private.

6.3 Students should also be aware that the CEO is able to monitor their use of the Internet when accessed through their school network. This includes the Internet sites and content accessed and the length of time spent using the Internet. Appropriate notices are included in Attachment C.

6.4 Monitoring of devices will occur regardless of whether the device was provided by the school, purchased by parents as part of a school initiative or individually owned.

7. Social Media

7.1 Whilst at school or using the school network on a school or personal electronic device, students must only access or contribute to social media sites if those sites are solely related to an educational context and if permission is given by a teacher to access those sites. This use must be in accordance with all other requirements specified in this Policy.

7.2 During personal use of social media, students must not communicate with their teachers or invite teachers to join in their personal networks.

7.3 Irrespective of whether teacher permission has been given to access a social media site, students must not:

- post any information about or images or videos of their teachers, themselves or other students, nor make comments about their school that might indicate that they are representing their school or that might bring their school into disrepute.
- forward on information, pictures, films or web links that contain inappropriate or hurtful material about members of the school community.
- sign up to sites that are hateful, racist, obscene, hurtful or contain inappropriate material.
- post information about themselves or another member of the school community that could be used to identify them (such as passwords, phone numbers and addresses) without carefully considering the possible unwanted consequences and, if in doubt, without first talking to a teacher.

- upload any images of themselves or another member of the school community where they are partaking in illegal activities.
- upload any images of Catholic Education Office students engaged in School activities without consent from a teacher and from all individuals in the photograph.
- upload any images of themselves or other students in uniform or otherwise identified with the school unless written permission has been received from the Principal.

References

Citizenship in the Digital Age – sample lesson plans

http://schools.nyc.gov/NR/rdonlyres/3CA0188D-66A2-490C-9E90-1EFCADA92F8C/0/Citizenshipinthedigitalage.pdf

Cybersafety Information and Advice

http://www.cybersmart.gov.au

Google Apps for Education

https://www.google.com/enterprise/apps/education/benefits.html

Forms

Attachment A: Acceptable Use Agreement

Attachment B: Personal Device Use Agreement

Attachment C: Workplace Surveillance Notices

Approved By:	Service Area Leadership Team
Issuing Service Area:	Information, Communication and Learning Technology Services
Implementation Date:	November 2013
Policy Revision Date:	June 2014
CEO Contact Officer:	Chief Officer, IC&LT Services
TRIM Record Number:	R187610

Attachment A

Archdiocese of Canberra and Goulburn
Catholic Education Office
Example of Student Acceptable Use Agreement

To have access to Information and Communication Technologies at _____ (school name) you need to follow these agreed practices.

Student Agreement

Using Information and Communication Technologies at school is a privilege. I have conditions to follow, which are for the safety and privacy of myself and others.

I will:

- Treat the school's ICT equipment with care and use it responsibly for educational purposes.
- Use the computers and Internet as instructed by my teacher(s).
- If I find inappropriate material, turn off the monitor and then tell my teacher or another adult immediately.
- Publish work and send emails using language I know is acceptable in my school.
- Tell the teacher if I receive a message that makes me feel uncomfortable.
- Respect the privacy of all computer users at school by correctly using passwords, and opening only my own work and emails.
- Be aware that it may not be possible to delete items stored on social media sites.

I will not:

- Give out any personal information that could be used to identify me, my family or friends, such as my surname, address, phone number or photo of myself, my parents or any other person while using the Internet.
- Pretend to be another person when communicating on the Internet.
- Break copyright law by copying and/or using another person's work.
- Write or send messages that would make another person feel uncomfortable.
- Pass on information with or about inappropriate material to other students.
- Waste materials through excessive printing or downloading.
- Misuse the Internet or encourage others to do so.
- Download or install any software or store files on my school's computer facilities without the permission of a teacher.
- Use the school's network for commercial purposes.
- Access a social media site on any device at school without the permission of a teacher.
- During personal use of social media sites communicate with my teachers or invite teachers to join my personal networks.
- Post any images, videos or comments about any member of my school community that might indicate I am representing the school or that might give my school a bad name or offend any member of the school community.
- Upload any images of other members of the school community without their permission.
- Upload any images of myself or other students in uniform or identified with the school in any other way without the permission of the Principal.

Student's signature (Year 3 and above)_____

Name (print):_____ Date:_____

Breaking the Student Agreement

If a student breaks the Student Agreement a number of steps can be taken:

- Withdrawal of individual log-on to an intranet and/or the Internet for a period of time as deemed appropriate.
- Parents notified.
- Appropriate ICT rights withdrawn.
- Guidance from the Learning Technologies Specialist/ICT Coordinator or School Executive as to how to avoid future problems.
- Steps as outlined in the School's Behaviour Management Policy.

Parent Acknowledgement

I give permission for my son/daughter _____(name) in_____(class) to use the Internet and other ICT facilities and I:

- have read the accompanying Acceptable Use Policy and the Student Agreement.
- agree to my child using Information and Communication Technologies for educational purposes in the manner outlined in the Policy.
- agree to my child transmitting work electronically to teachers and having the work published where the school considers that to be appropriate.
- have talked to my child about safety, privacy and copyright concerns when using computers at school and home.
- consent to my child's use of the School's student email system and other Google Apps on the understanding that the system is provided through Google Apps for Education and that consequently students' 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. Information about the security and privacy features of Google Apps for Education may be found at https://www.google.com/enterprise/apps/education/benefits.html

Parent/Guardian's signature: _____

Name (print) :_____Date:_____

Please return this form to school as soon as possible.

Your child will be unable to use the school's network or the Internet until this form is returned.

Thank you

Attachment B

Archdiocese of Canberra and Goulburn
Catholic Education Office
Example of Personal Electronic Device Acceptable Use Agreement

To have access to the computer network at _____ (school name) with a personal electronic device of your own, such as a laptop, tablet, smart phone or wifi-enabled storage device, you need to follow these agreed practices, in addition to having agreed to the conditions in the Acceptable Use Agreement for use of your school's computer facilities and external networks. You should not bring any of these devices to school without the Principal's approval.

Student Agreement

I will:

- Only use personal electronic devices that have been approved by my school for use on the school's network.
- Follow all the conditions I have agreed to in the Acceptable Use Agreement for use of my school's computer facilities and external networks when using an approved personal electronic device.
- Only access the Internet at school through the school's wireless network.
- Follow all instructions given by a teacher about my personal electronic device, including turning off the device or handing over the device to the teacher on request, and only using approved applications on the device.
- Be responsible for maintaining my personal electronic device, including keeping the battery charged, and purchasing and upgrading software

I will not

- Whilst at school lend my device to others and I will ensure that it is stored securely when not in use.
- Whilst at school use my device to take photographs or record video or sound without the permission of a teacher and all the people being photographed or recorded.

Student's signature_____

Name (print):_____ Date:_____

Breaking the Personal Device Acceptable Use Agreement

In addition to the consequences described in the Acceptable Use Agreement for use of school computer facilities and external networks, students may be banned from taking their personal electronic device to school and/or using it on the school computer network.

Parent Acknowledgement

I give permission for my son/daughter _____(name) in_____(class) to use a personal _____ (device type) at school and on the school's computer network and I:

- have signed the accompanying Acceptable Use Agreement for use of the school's computing facilities and external networks.
- agree that, whilst all normal care will be taken, the school is in no way responsible for replacement of the device due to theft, repairs due to breakage or any other sort of maintenance of the device.
- recognise that, whilst every reasonable attempt will be made to enable the device to access the school's computer network, there is no guarantee that this will be possible. The school is limited to devices that are supported by the CEO on its networks.
- acknowledge that my child's use of the device at school will at all times be subject to the directions of teachers and that failure to follow those directions may lead to the consequences described above.

Parent/Guardian's signature: _____

Name (print) :_____Date:_____

Please return this form to school as soon as possible.

Your child will be unable to use the personal device at school until this form is returned.

Thank you

Attachment C

WORKPLACE SURVEILLANCE NOTICE (NSW)

All messages on the CEO's system will be treated as business or education related messages which may be monitored. Accordingly you should not expect that any information or document transmitted or stored on the CEO's computer facilities and external networks will be private.

From time to time the content and usage of email may be examined by the CEO or the School Principal or a third party on the CEO's behalf. This will include electronic communications which are sent to you or by you, both internally and externally.

You should also be aware that the CEO is able to monitor your use of the internet, both during working hours and outside of those hours. This includes the internet sites and content that you access and the length of time you spend using the internet.

CEO monitoring of its computer facilities and external networks is ongoing and is consistent with the *Workplace Surveillance Act 2005* (NSW).

WORKPLACE SURVEILLANCE NOTICE (ACT)

All messages on the CEO's system will be treated as business or education related messages which may be monitored. Accordingly you should not expect that any information or document transmitted or stored on the CEO's Computer Facilities and External Networks will be private.

From time to time the content and usage of email may be examined by the Principal or the CEO or by a third party on the CEO's behalf. This will include electronic communications which are sent to you or by you, both internally and externally.

You should also be aware that the CEO is able to monitor your use of the internet, both during working hours and outside of those hours. This includes the internet sites and content that you access and the length of time you spend using the internet.

CEO monitoring of its Computer Facilities and External Networks is ongoing and is consistent with the *Workplace Privacy Act 2011* (ACT).