Computer Facilities and External Networks – Acceptable Use

Related Policies

Copyright
Privacy
Teaching in Catholic Schools – A Statement of Principles

Purpose

This policy describes and facilitates the acceptable use of Catholic Education Office (CEO) computer facilities and external networks including the internet.

Policy

School Principals and other CEO workplace managers are responsible for establishing and maintaining on-site procedures for a secure computing environment with regard to authorised access, student supervision and Acceptable Use by staff and students consistent with the core business and functions of the CEO and its system of schools.

All CEO workplaces are required to implement the attached CEO User’s Code of Practice.

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 the employee’s work duties and performance, with system operations or other system users.

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

Devices include but are not limited to laptops, 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.

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

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

Licensed Software collectively refers to copyrighted and proprietary programs, data and documentation.
Notice of Surveillance is a notice required in NSW workplaces by the Workplace Surveillance Act 2005 (NSW). The Notice of Surveillance must include:

a) the kind of surveillance to be carried out (camera, computer or tracking), and  
b) how the surveillance will be carried out, and  
c) when the surveillance will start, and  
d) whether the surveillance will be continuous or intermittent, and  
e) whether the surveillance will be for a specific limited period or ongoing.

A suggested notice is provided with this policy at Attachment B.

Procedures

1. The CEO will:

1.1 ensure that the authorised use of computer facilities and external networks, including the internet, by its users relates to CEO business and is consistent with principles, regulations and laws relating to the privacy and safety of school students and CEO staff;  
1.2 provide appropriate software, either onsite or by the service provider, to allow access to appropriate online sites only;  
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 network;  
1.5 take such lawful action as it deems necessary to fulfil its duty of care to users including the blocking of internet sites, restricting a user’s access and the confiscation of devices;  
1.6 consider applications to allow the school's computer system to be used for other purposes so long as the proposed activity does not contravene CEO Policy or adversely impact on the performance of work duties.

2. CEO Heads of Service will:

2.1 implement the CEO User’s Code of Practice;  
2.2 provide appropriate training and instruction which ensures that all users understand and agree to comply with Codes of Practice;  
2.3 monitor the use of CEO Computer Facilities And External Networks and inform users by Notice of Surveillance that this monitoring occurs;  
2.4 investigate and reach a finding regarding any alleged breach of the User’s Code of Practice by employees.

3. School Principals will:

3.1 implement the CEO User’s Code of Practice for staff including volunteers and contractors;  
3.2 develop and implement an appropriate Student Code of Practice or Acceptable Use Agreement;  
3.3 provide appropriate training and instruction which ensures that all users understand and agree to comply with Codes of Practice;
3.4 provide education programs that focus on ethical and acceptable uses of the Internet as well as appropriate online etiquette;

3.5 provide education programs for teachers and students which develop protective behaviours when working and accessing online environments;

3.6 ensure that student access will be appropriately supervised and that alleged breaches of the Code of Practice by students are investigated and a finding reached;

3.7 highlight to users the possible dangers of communicating personal information on the internet;

3.8 obtain written permission from students 18 years and over or obtain from the person with parental responsibility, annual written permission for students under 18 years of age, to publish or transmit student work which may or may not include identifying student information. This includes any publishing of student work which may be done by a third party on their behalf;

3.9 monitor the use of its Computer Facilities and External Networks and inform users that this monitoring occurs.

3.10 provide systems and procedures to protect users from offensive material.

4. All users will:

4.1 obtain authorisation prior to using CEO computer facilities and external networks, including the internet, through the use of one’s own personal passwords and user identification;

4.2 be aware that software (licensed, shareware, freeware, evaluation or otherwise) including system software, application software or data files, may only be downloaded and/or installed in accordance with the instructions provided by the Catholic Education Office ICT Services and/or the school’s authorised personnel

4.3 only use CEO computer facilities and external networks for acceptable use and in accordance with this policy, other relevant policies and the Code of Practice;

4.4 respect and maintain the confidentiality of information stored on CEO computer facilities and external networks;

4.5 take reasonable steps to protect the personal information stored on CEO computer facilities and external networks from misuse and unauthorised access;

4.6 immediately report:

   4.6.1 any breach of security, confidentiality or privacy;
   4.6.2 receipt or accidental download of inappropriate or offensive material;
   4.6.3 receipt or presence of any virus;
   4.6.4 any breach or alleged breach of the Code of Practice.

5. Use of Devices

5.1 Staff choosing to authenticate a personal owned notebook or other approved device to the schools network must sign an end user agreement that outlines the level and type of support available and the end user’s responsibility in managing the notebook or device.
5.2 Devices owned or used by staff or students may be searched and / or confiscated if the Service Head or 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, serious breach of policy or serious breach of the relevant Code of Conduct or Code of Practice.

6. Monitoring

From time to time the content and usage of email may be examined by 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.

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 CEO’s computer facilities and external networks will be private.

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.

References

Diocese of Maitland – Newcastle: Draft Workplace Internet Email & Network Usage Policy

Forms

Archdiocese of Canberra and Goulburn Catholic Education Office – User’s Code of Practice – Acceptable Use of Computer Facilities and External Networks (see below)

Archdiocese of Canberra and Goulburn Catholic Education Office – Sample Primary School - Student Acceptable Use Agreement for Access to ICT (see below).
ACCEPTABLE USE OF COMPUTER FACILITIES AND EXTERNAL NETWORKS

Purpose
This Code of Practice has been developed for all non-student users of the CEO’s Computer Facilities and External Networks and is consistent with the CEO’s policy on Acceptable Use of Computer Facilities and External Networks.

MANDATORY PROCEDURES

Security
- Ensure your login and password are unique (i.e. don’t use shared passwords).
- Log your workstation off the network before leaving the workstation.
- Ensure devices that join the network or are brought onto CEO / school property or to sanctioned school activities do not contain content or are used in any way that is in breach of the Acceptable Use of Computer Facilities and External Networks policy.
  (NB Devices include but are not limited to laptops, iPods, USB storage devices and mobile phones).

Supervision of Students
- Student activity on computer networks will be supervised appropriately by staff. Staff will take all reasonable steps to ensure that student activity on networks is in accordance with the School’s Code of Practice for Students.

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 the employee’s work duties and performance, system operations or other system users.

Unacceptable Use means to do or omit to do anything which would breach the law, CEO / School Policies or your employment contract. For example it is unacceptable to:
- Abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other).
- Send or receive or download obscene or pornographic material.
- Injure the reputation of the CEO and its system of schools or to do or omit to do anything that may cause embarrassment to the CEO and its system of schools.
- Spam or mass mail or to send or forward chain mail letters.
- Infringe the copyright or other intellectual property rights of another person.
- Perform any other unlawful or inappropriate act.
- Download video files or downstream from the internet for purposes inconsistent with the CEO’s core business.
- Communicate information concerning any password, identifying code, personal identification code or other confidential information.
- Game, wage or bet.
- Perform personal business activity for financial gain or commercial purposes.

Employees of the Archdiocese of Canberra and Goulburn Catholic Education Office may access the Internet via the CEO Local and /or Wide Area Network after signing the following declaration.

I declare that I have read and I understand the Archdiocese of Canberra and Goulburn CEO’s policy on Acceptable Use of Computer Facilities and External Networks and the accompanying User’s Code of Practice. I understand that my use of the CEO’s Computer Facilities and External Networks may be monitored.

Surname: __________________________ Given Name: __________________________
Location: __________________________ Position: __________________________
Signature: __________________________ Date: ______/____/____

PLEASE RETAIN A COPY FOR YOUR RECORDS
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 documented transmitted or stored on 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 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 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 documented transmitted or stored on 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 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.
Example of Student Acceptable Use Agreement

To have access to Information and Communication Technologies at ______________ 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 the way my teacher has asked me to.
• If I find something that is not appropriate for primary school children on the Internet I will turn off the monitor, 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.
• Pack away equipment and tidy the area I was using.

I will not:
• Give out my personal information, such as my surname, address, phone number or photo of myself, my parents or any other person while using the internet.
• Break copyright law by copying and/or using another’s work.
• Write or send messages that would make another person feel uncomfortable.
• Pass on information about inappropriate material to other students.
• Waste materials through excessive printing or downloading.
• Misuse the Internet or encourage others to do so.

Breaking the Student Agreement

If a student breaks the Student Agreement a number of steps can be taken:
• Withdrawal of individual log-on to intranet, internet or both 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 Behaviour Management Policy.

Parent Acknowledgement

I give/do not give (circle one) permission for my son/daughter ___________________ in ________ 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.
• Have talked to my child about safety, privacy and copyright concerns when using computers at school and home.

Parent’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