SUBMISSION No. 8

Archdiocese of Canberra and Goulburn
CATHOLIC EDUCATION OFFICE

Director

PO Box 3317
Manuka ACT 2603
Telephone (02) 6234 5455
Facsimile (02) 6239 6567
director@cg.catholic.edu.au
www.ceocg.catholic.edu.au
ABN: 47824127996

File Ref: 2009/93:R52750

15 June 2010

Mr Jerome Brown
A/g Committee Secretary
Joint Select Committee on Cyber-Safety
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Mr Brown

RE: INQUIRY INTO CYBER-SAFETY

In response to your letter of 14 May 2010 to Mr Brian Croke, Executive Director, Catholic Education Commission NSW concerning the Australian Parliament's Joint Select Committee Inquiry into Cyber Safety, please find below the submission from the Catholic Education Office for the Archdiocese of Canberra and Goulburn into how to reduce the risk to young people engaging in ICT technologies.

1. Current online environment engaged by children

- Students engage a range of online environments as part of the school curriculum in classrooms and other specified school learning areas. Students also engage a range of online environments outside of the immediate school context for social and/or school related purposes.
- School based online usage by student in system schools in the Archdiocese of Canberra and Goulburn is informed by system (Catholic Education Office) policies including: Privacy Policy (based on National Privacy Principles); and the Computer Facilities and External Networks – Acceptable Use Policy. School online practices are also based on the system's Code of Professional Practice and use of exemplar support documents; for example, the 'Student Acceptable Use Agreement', including a specific parent acknowledgement component.
- Principals ensure alignment to relevant system policies and implement school based procedures to effect system policy; for example, acceptable practices for mobile phone usage.
- Access to inappropriate sites at schools is prevented through a range of system and school level filtering and monitoring processes. Parents are supported in their responsibility to supervise their child's home online access through school based education forums.

2. Abuse of children online

- Incidents of child abuse; for example, cyber bullying are dealt with by school and system personnel in accord with relevant legislation, policy and procedures. Low risk behaviours and incidents are usually dealt with at school level.

- Incidents of a significant nature, for example, those involving allegations of inappropriate student behaviour reported to the Police, are formally investigated by school and/or system personnel.

3. Inappropriate online social and health behaviours involving children

- Student online behaviour is monitored closely at school level in accord with policy and school practices.
- Parents are involved in school based discussions and interventions where children are demonstrating significant, ongoing online behaviours of concern.
- The delivery of school curriculum is very responsive in the teaching of pro-social skills regarding the range of pernicious behaviours and thinking that children are subject to; for example, substance abuse and other addictive/anti-social behaviours.
- Resources that are regularly used in schools to teach pro-social behaviours include the programs, frameworks and activities on the following web sites: http://bullyingnoway.com.au/; http://www.cybersmart.gov.au; http://www.ncab.org.au.
- Schools and system staffs contribute to the development and implementation of national frameworks and processes in response to student needs. These include, for example, the National Safe and Supportive Schools Framework, Kids Matter and Mind Matters.

4. Identity theft

- Low level identity theft related matters; for example, a student inappropriately accessing and using another student's password is generally managed at school.

5. Breaches of privacy

- As with matters of identity theft, a breach of privacy by a student is initially managed at school level through the Principal. Serious matters, some involving police investigation, are investigated and managed by the Principal and system personnel. Appropriate records are kept for serious offences in keeping with relevant legislation requirements.

6. & 7. Responses to cyber-safety threats and cooperation with stakeholders

- The Catholic Education Office has a designated service area which ensures cyber safety surveillance on behalf of the system and system schools.

- The system is also part of a range of inter-diocesan and inter-system networks to assure cooperation and collaboration regarding matters of cyber-safety in the schooling domain.

8. Supports for schools for cultural change re cyber-bullying

- Policies and programs (described in 1 and 3 above) are promulgated and supported at system and individual school level.
- The system is working on a range of initiatives to develop a school and system wide student wellbeing focus; for example, that relating to the *Positive Behaviour Support, Positive Partnerships* and *Quality Teaching Framework* programs.

9. Role of parents, families, carers and community

- Parents and relevant community members are provided with information; for example, through system policy access and school based newsletters and through opportunities such as system and school presentations and workshops to assist them fulfil their respective responsibilities regarding cyber-safety.
- Parents and relevant community members are involved as collaborative participants and decision makers in policy development affecting all matters of student well being and safety; for example, locally via the School Board or School Community Council, and at system level through membership of the Catholic Education Commission for the Archdiocese of Canberra and Goulburn.

Contact officer on this matter is Mr Michael Traynor, Senor Officer: Human Resources – Personnel, phone 02 6234 5437, email michael.traynor.cg.catholic.edu.au.

Yours sincerely

Moira Najdecki
Director