POLICY

CYBERBULLYING

RELATED POLICIES

TCEC Anti-Discrimination, Harassment & Bullying Policy (2007)
TCEC Code of Conduct (2006)
TCEO Computer Usage Policy (2009)

Adopted by:
St. Brigid's Catholic School, New Norfolk

First Implemented February 2012
Last review October 2013

CYBERBULLYING POLICY

RELATED DOCUMENTS

TCEC Anti-Discrimination, Harassment & Bullying Policy (2007)
TCEO Computer Usage Policy (2009)
TCEC Code of Conduct (2006)

RATIONALE

Catholic schools and offices have a responsibility to provide educational and workplace environments that promote the dignity and respect of everyone within their organisations and therefore must aim to eliminate bullying in all of its forms.

Cyberbullying, like all other forms of bullying, must therefore not be tolerated in our places of work for it has a negative impact on all who are touched by it. It adversely affects student learning outcomes. It erodes the rights and the physical, emotional, psychological, spiritual and social wellbeing of individuals. It lowers workplace morale for it can interfere with the effectiveness of work and learning environments by making them hostile, unpleasant and offensive places.

Thus, the purpose of this policy is to articulate the rights and responsibilities of all in the Catholic education sector with regards to cyberbullying and, by doing so, to continue the growth of Catholic school communities that:

- Respond to human need with compassion, fairness and justice that respects the dignity of all;
- Create an inclusive environment that values and respects diversity, equity and subsidiarity; and
- Build and sustain relationships based on Gospel values that are life-giving and empowering.

TCEC Mission Statement (2006)

This policy should be read in conjunction with the TCEC's *Anti-Discrimination, Harassment and Bullying Policy* (2007).

DEFINITIONS

Cyberbullying — Cyberbullying involves the use of information and communication technologies to support deliberate,

repeated, and hostile behaviour by an individual or group, that is intended to harm others.*

Bill Belsey
(The creator of the world's first website about the issue of cyberbullying – www.cyberbullying.org)

Notes:

While cyberbullying is similar to real life bullying, it also differs in the following ways:

- It can be difficult to escape and is invasive for it can occur 24/7 and a person can be targeted at home or, indeed, almost anywhere.
- It can involve harmful material being widely and rapidly disseminated to a large audience, for example, rumours and images can be posted on public forums or sent to many people at the 'press of a button'.
- It can provide the bully with a sense of relative anonymity and distance from the victim so there is a lack of immediate feedback or consequences.

Cyberbullying might occur over the Internet, in instant messaging (IM), chat rooms / bash boards, social networking sites, blogs, gaming sites, over the phone by SMS or MMS, by email or via other technologies.

Please refer to Appendix 1 for more detailed examples of cyberbullying behaviour.

POLICY

When addressing issues of cyberbullying, all Catholic systemic school authorities will consistently apply the principles and procedures contained within this policy document.

In regard to this policy, the TCEO recognises its responsibility to ensure that the rights of employees, students and volunteers to be physically, emotionally and psychologically safe in, or in activities associated with, their relevant school or office workplace, will be protected. This responsibility may extend to beyond school / workplace-based online behaviour where such behaviour impacting harmfully upon students, staff and volunteers becomes known.

Cyberbullying will not be tolerated in Catholic systemic schools or workplaces.

* This definition has been adopted by the Federal Government's Australian Communications and Media Authority (ACMA).

PRINCIPLES

General Principles:

This policy has been formulated on the basis of the following **general** principles:

1. Employers / their delegates owe a duty of care to their employees, to students and to all others who work in or visit schools / workplaces.

2. Cyberbullying within workplaces is to be handled in a straightforward, effective, sympathetic, timely and fair manner.

3. Compliance with all relevant legislation covering issues of cyberbullying must be ensured.

4. Avenues for improved interpersonal relationship and conflict resolution are to be provided where practicable.

5. Ethical and professional conduct and standards of behaviour for employees are to be promoted.

6. Principals and senior staff members are to be appropriately supported in the performance of their human resource management functions.

7. All individuals affected by the experience of cyberbullying are to be provided with an avenue to discuss a grievance and explore a choice of actions where practicable.

8. A deliberate and ongoing focus in schools and workplaces must be placed on promoting positive online behaviour. This will incorporate the development of positive, appropriate and constructive online relationships with peers, colleagues, family, friends and appropriate others in a variety of media encompassing concepts such as netiquette, appropriate contact and communication with others, cyberbullying itself, problematic usage and unethical behaviour.

Specific Principles:

In addition, this policy has been formulated on the basis of the **specific** principles that apply to cases of cyberbullying which demand more formalised responses. Appendix 2 of this policy will provide details of these specific principles drawn from the list below:

1. Due process
2. Natural justice
3. Confidentiality
4. Complaints
5. Resolution

GUIDELINES

1. Cyberbullying – a serious matter:

1.1 Employers / their delegates have a duty of care to protect all in their communities from cyberbullying and failure to 'take reasonable care' could amount to charges of negligence being laid and sustained.

1.2 Duty of care can extend outside of normal school or workplace hours where a school / workplace authority or an individual employee is aware or becomes aware that a child / employee / other person may be harmed (see Appendix 3).

1.3 Employers / their delegates must effectively inform their stakeholders that engaging in cyberbullying may mean facing serious consequences including an individual being the subject of a Police investigation into a criminal offence.

1.4 For TCEO employees, cyberbullying is a breach of the TCEC's *Code of Conduct* (2006) and such behaviour may draw sanctions as serious as dismissal and the laying of criminal charges or civil court action.

1.5. In order to limit the occurrence of such serious situations as articulated in the above (1.1–1.4), the TCEO will provide relevant and appropriate professional learning experiences on cyberbullying to schools statewide via the ICT Coordinators' Network meetings and where appropriate or necessary through Principals' state-wide and / or regional meetings.

1.6 Local school communities would be expected to continue the educative process (in 1.5 above) with students in their schools as well as with parents who share with the school responsibility for such matters. For parents, this could be in forms such as information evenings and afternoon student-parent sessions.

2. School / workplace cyberbullying policies:

2.1 In order to help manage risk, protect users and protect the organization, Catholic systemic schools and related workplaces are required to put in place a range of local technology usage policies, one of which is the Cyberbullying Policy. This policy will be promulgated and effectively communicated to all stakeholders in the school / workplace community. It is expected that the effective and appropriate monitoring of workplace practices relevant to the Policy will be ongoing. This Policy should remain accessible to all stakeholders in the workplace.

2.2 An 'Acceptable Use Policy' concerning a commitment to the appropriate use of all technologies available in a school / workplace should be signed off annually by individual students / employees / relevant others.

3. Recommended strategies for individuals to respond to instances of cyberbullying:

3.1 The following general strategies are recommended to assist those who are victims of cyberbullying activity:

3.1.1 Report any incidence of cyberbullying or upsetting hostile cyberspace behaviour, including deliberate exclusion, to a relevant parent, trusted adult, line manager or school / workplace authority.

3.1.2 Do not respond to further messages / postings from the bully and, if possible, block their mobile phone number or email address.

3.1.3 Keep evidence of any cyberbullying (including screen captures, the bully's screen name, text and images) to assist in tracking down the bully and as necessary reporting the matter to Police.

3.1.4 Report any concerns to the administrator of the service used for bullying whether this be the mobile phone provider if SMS is involved, the website administrator or internet service provider if social networking or chat services are the vehicles for the cyberbullying occurring.

3.1.5 Seek support from an appropriate and supportive contact such as the school counselor or chaplain (for children) or from a professional colleague / workplace authority (for adults).

3.1.6 Contact Police immediately in cases of possible serious threats to life or physical wellbeing or where a child protection offence (e.g. child pornography, grooming) has occurred.

See APPENDIX 3 for a summary of recommended responses to instances of cyberbullying.

REFERENCES

Butler, D., Kift, S., Campbell, M. (2009) – *Cyber Bullying in Schools and the Law: Is there an effective means of addressing the power imbalance?* - eLaw Journal: Murdock University Electronic Journal of Law (2009) 16 (1).

TCEC *Anti-Discrimination, Harassment & Bullying Policy* (2007)

TCEC *Code of Conduct* (2006)

TCEC *Taking Care Policy* (2005)

See APPENDIX 4 for details of Commonwealth and State Government laws which cover cyber crime (incorporating cyberbullying).

FORMS

Nil

APPENDICES

APPENDIX 1	What is Cyberbullying?
APPENDIX 2	Specific Principles that Apply in Responding to Cyberbullying
APPENDIX 3	Summary of Direct Action Options for Schools or TCEO Workplaces when Dealing with Cyberbullies
APPENDIX 4	State and Commonwealth Government Laws and Cyber Crime

APPENDIX 1

WHAT IS CYBERBULLYING?

(adapted from the Archdiocese of Sydney's *'Dealing with Cyberbullying'* Operational Draft August 2008)

Cyberbullying can include, but is not limited to, the items listed below. This list outlines the types of cyber behaviour that are not consistent with this Cyberbullying Policy nor are they consistent with Acceptable Use policies across the full range of systemic Catholic schools and workplaces in the state.

- Email:

  Sending harassing, threatening and / or menacing messages to targets either directly, anonymously or using another person's address or alias.

- Instant Messaging (IM):
  (systems include MSN Messenger, Yahoo and Bebo)

  Harassing someone or having heated arguments (called 'flaming') in private chat rooms with the use of inappropriate / obscene language.

- Chat Rooms / Bash Boards:

  Allowing students / others to anonymously write / create anything (true or untrue) or add cruel comments about someone in a world wide forum.

- Short Text Messages (SMS):

  Masquerading as someone else and using that person's mobile phone or computer to send harassing or threatening messages.

- Websites / Social Networking sites:

  Mocking, teasing and harassing online, or voting online for the 'ugliest' / 'fattest' / 'dumbest' (etc.) person, or posting visuals that can be altered (including sexually explicit material).

APPENDIX 2

SPECIFIC PRINCIPLES THAT APPLY IN RESPONDING TO CYBERBULLYING

(adapted from the TCEC *Anti-Discrimination, Harassment & Bullying Policy* 2007)

1. **Due Process**: This is based on the concept of procedural fairness. It includes an individual's right to be adequately notified of complaints, charges or proceedings involving him / her, and the opportunity to be heard at these proceedings. Due process incorporates principles of natural justice.

2. **Natural Justice**: The principles of natural justice apply at all stages of the complaint resolution process.

   Key elements of natural justice covered in this policy include:

   2.1 All individuals must be given a fair opportunity to understand the case against them, have sufficient time to provide their views on the matters put to them, and to be heard.

   2.2 All parties to a decision should be heard, and all relevant arguments be considered before a decision is made.

   2.3 People should have an opportunity to respond to any adverse material that may influence a decision affecting them.

   2.4 People should know about decisions or judgements that affect them.

   2.5 Decision-makers must act fairly and without actual or perceived bias.

   2.6 Persons using this policy must not be victimised and have the right to take action under this policy, or via such agencies as the Anti-Discrimination Commission, if they believe victimisation has occurred.

3. **Confidentiality:** Confidentiality is to be maintained as far as practicable during resolution procedures but there may be times when disclosure of information contained in a complaint or a response to a complaint is appropriate.

3.1 The public interest may require that the employer releases confidential information to the appropriate outside authorities and this is permitted by law in certain circumstances. Similarly the employer must comply with binding legal requirements to release confidential information, for example in response to a subpoena or a search warrant.

3.2 Communication about the complaint must be limited to persons to whom disclosure is consistent with their official position and responsibilities under this policy. Only those staff with responsibility to investigate and/or resolve matters of cyberbullying will have access to the relevant material. However, in fairness to those persons who are the subject of cyberbullying complaints, the investigator must provide them with sufficient information and an opportunity to respond adequately to the complaint.

3.3 All persons participating in the investigation are required to keep their involvement confidential. However, while all attempts will be made to honour the wishes of the person who makes a complaint, in some circumstances, the seriousness of the allegations raised will mean that Principals and supervisors are under a legal obligation to ensure that the matter is investigated beyond that which the person who is the subject of the complaint may originally envisage. This is to ensure that the employer fulfils its duty to maintain a physically and psychologically safe workplace environment for all.

4. **Complaints**: Complaints may relate to minor transgressions and informal resolution may be possible, or to more serious issues where formal processes may be needed.

5. **Resolution**: Where possible, complaints should be resolved at the lowest possible organisational level by open dialogue, cooperation and/or mediation (a voluntary process), which aims to assist the parties to reach an acceptable outcome. An individual may choose to resolve the problem by discussing it with the other party or parties concerned. This may involve the assistance of others and the school/TCEO Grievance Policy must be followed in the first instance. A process for investigation of a formal complaint is available where discussion and/or mediation is inappropriate or has proved unsatisfactory. If in the case of employees serious misconduct is alleged, then the matter will be dealt with according to the *Taking Care* policy and procedures.

APPENDIX 3

SUMMARY OF DIRECT ACTION OPTIONS FOR SCHOOLS OR TCEO WORKPLACES WHEN DEALING WITH CYBERBULLIES

Where the cyberbullying contains …	… then the action to be taken <u>may</u> include …	… and responsibility for such action lies with the …
Bullying	(If perpetrated by a student) ▪ Contacting parents ▪ Suspending / expelling / taking other action (according to school &/or system policies) ▪ Counselling	▪ PRINCIPAL / PRINCIPAL'S DELEGATE (e.g. DP, AP) *… who may choose to notify the Regional Director (according to the seriousness of the incident/s)*
	(If perpetrated by an employee) ▪ Activating *Taking Care* Policy ▪ Activating processes in *Anti-Discrimination, Harassment and Bullying Policy* ▪ Counselling	▪ PRINCIPAL (for school employees) *… who notifies Regional Director (as appropriate, advice given to Principal) who in turn may choose to notify the Director TCEO (according to the seriousness of the incident/s)* ▪ DIRECTOR TCEO (for TCEO employees)
	(If perpetrated by other than a student / employee) ▪ Contacting Police ▪ Contacting relevant others	▪ PRINCIPAL (for school-based offences) *… who notifies Regional Director (as appropriate, advice given to Principal) who in turn may choose to notify the Director TCEO (according to the seriousness of the incident/s)* ▪ DIRECTOR TCEO (for TCEO-based offences)
Overt sexual content	(If perpetrated by a student) ▪ Contacting Police ▪ Contacting Child Protection authorities ▪ Contacting parents ▪ Suspending / taking other action (according to school &/or system policies) ▪ Counselling	▪ PRINCIPAL *… who notifies Regional Director who in turn notifies Director TCEO (as appropriate, advice given to Principal)*
	(If perpetrated by an employee) ▪ Contacting Police ▪ Activating *Taking Care* Policy ▪ Counselling	▪ PRINCIPAL (for school employees) *… who notifies Regional Director who in turn notifies Director TCEO (as appropriate, advice given to Principal)* ▪ DIRECTOR TCEO (for TCEO employees)
	(If perpetrated by other than a student / employee) ▪ Contacting Police	▪ PRINCIPAL (for school-based offences) *… who notifies Regional Director who in turn notifies Director TCEO (as appropriate, advice given to Principal)* ▪ DIRECTOR TCEO (for TCEO-based offences)
Threats to life / sexual assault / child protection offences / other criminal activity	(If perpetrated by a student) ▪ Contacting Police (mandatory) ▪ Contacting Child Protection authorities ▪ Contacting parents ▪ Suspending / expelling / taking other action (according to school &/or system policies) ▪ Counselling	▪ PRINCIPAL *… who notifies Regional Director who in turn notifies Director TCEO (as appropriate, advice given to Principal)* *… who then steps back and allows Police investigation to run its course* *… who then considers school / system response according to policy should the Police investigation find no case to answer*
	(If perpetrated by an employee) ▪ Contacting Police (mandatory) ▪ Activating *Taking Care* Policy ▪ Counselling	▪ PRINCIPAL (for school employees) *… who notifies Regional Director who in turn notifies Director TCEO (as appropriate, advice given to Principal)* *… who then steps back and allows Police investigation to run its course* ▪ DIRECTOR TCEO (for TCEO employees) *… who then steps back and allows Police investigation to run its course* *… who then considers system response according to policy should the Police investigation find no case to answer*
	(If perpetrated by other than a student / employee) ▪ Contacting Police (mandatory)	▪ PRINCIPAL (for school-based offences) *… who notifies Regional Director who in turn notifies Director TCEO (as appropriate, advice given to Principal)* *… who then steps back and allows Police investigation to run its course* ▪ DIRECTOR TCEO (for TCEO-based offences) *… who then steps back and allows Police investigation to run its course*

NOTE

Where a school / workplace authority or an individual employee is aware, or becomes aware, that a child / employee / other person is experiencing cyberbullying outside of normal school / workplace hours, then duty of care can extend to these times (from both a legal and moral perspective) and may demand that the matter be addressed either through direct action or through escalation.

APPENDIX 4

STATE & COMMONWEALTH GOVERNMENT LAWS AND CYBER CRIME

The numerous State and Commonwealth Government laws which cover cyber crime include:

- Commonwealth Government Criminal Code Act 1995.
  Section 4.7.4.17

  It is an offence for a person to use *a carriage service to menace, harass or cause offence*.

- Commonwealth Government Criminal Code Act 1995.
  Section 4.7.4.15

  It is an offence for a person to use *a carriage service to make a threat*.

- Commonwealth Government Crimes Act 1914.
  Part VIIB, Section 85ZE

  It is an offence for *a person to knowingly or recklessly use a telecommunications service supplied by a carrier in such a way as would be regarded by reasonable persons being, in all circumstances, offensive*.

- Tasmanian Government Criminal Code Amendment (stalking) Bill 2004.

  It is an offence for a person to transmit offensive material and send electronic messages with the intention of causing physical or mental harm.

The sending of images is also covered by various State and Commonwealth Government laws that prevent the publication of material that is objectionable, unclassified or unsuitable for minors.