Policy name	Cyberbullying Policy and Procedure
Responsible person	CEO, Managers
Staff involved	All staff
Review dates	2018
Related documents	Legislation: Sex Discrimination Act (1984) (Com), Vic Equal Opportunity Act (2010) (Vic), Crimes Amendment (Bullying) Act 2011 (Vic), Federal Australian Human Rights and Equal Opportunity Commission Act (1986) (Com), Federal Racial Discrimination Act (1975) (Com), Federal Disability Discrimination Act (1992) (Com), Victorian Disability Act 2006 (Vic), The Victorian Occupational Health and Safety Act (2004) (Vic),The Commonwealth Criminal Code Act (1995) (Com), The Commonwealth Crimes Act (1914) (Com), The Victorian Crimes Act (1958) (Vic), Children, Youth and Families Act (CYFA) 2005, Child Wellbeing and Safety Act (2005), Commission for Children and Young People Act 2012, Charter of Human Rights and Responsibilities Act 2006 Policies: Complaints and Appeals Policy and Procedure, Privacy Policy and Procedure, Access and Equity Policy and Procedure, Harassment, Discrimination, Mandatory Reporting Policy & Procedure, Child Safe Policy & Procedure including Statement of Commitment), Victimisation and Bullying Policy & Procedure, Computers, Internet and E-mail Policy & Procedure; Social Media Policy and Procedure. Other: Codes of Conduct, DET Cyberbullying posters and bookmarks, VCAL Student Contract, VCAL Student Package, VCAL Teacher's Package, Australian Privacy Principles summary, DET Interactive Learning Modules at http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/bullystopmodules.aspx and http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/cyberbullying.aspx Student Wellbeing Hub https://studentwellbeinghub.edu.au/ Australian Government office of the children's eSafety Commissioner – https://www.esafety.gov.au/complaints-and-reporting/offensive-and-illegal-
	content-complaints/report-offensive-or-illegal-contentt Australian Communications and Media Authority (ACMA) http://www.acma.gov.au/

Policy Context

Information Communications Technologies (ICTs) are now very much a part of everyday life and learning. While ICTs brings new opportunities for learning, they also bring some risks.

This document was reviewed and accepted by the Board of Governance of the Wyndham Community and Education Centre Inc on 07/12/17 and supersedes all previous versions.

Version: 2017 v1 Document number: 372 Page 1 of 6 G:\2017\2017 Compliance_P&P_AQTF\Policies\Access equity\cyber bullying.docx

Cyberbullying is a criminal offence of the digital age, for any person above 14 years of age, where individuals are targeted through the use of technology. Cyberbullies can use the Internet, a mobile device or even a camera to harass, embarrass, threaten or hurt a person. The biggest concern here is that this type of bullying behaviour can easily be shared with a wide audience making it more widespread than traditional bullying.

Cyberbullying is direct verbal or indirect bullying behaviours that are offensive, intimidating, threatening or harassing using digital technologies against someone. This includes inappropriate communication via mobile devices, setting up a defamatory personal website or deliberately excluding someone from social networking spaces.

All forms of cyberbullying are unacceptable at Wyndham Community and Education Centre Inc. (Wyndham CEC). Such behaviour is unlawful and will not be tolerated. All staff, clients, volunteers and students have the right to an atmosphere free of cyberbullying and have the responsibility to prevent it and expose it when it occurs. Cyberbullying can detrimentally affect an individual's health and well-being. Wyndham CEC staff will report behaviour to Police if they think a crime has been committed.

What is Cyberbullying?

Cyberbullying is bullying behaviour that is carried out using digital technologies such as the Internet, email, chat rooms, discussion groups, online social networking sites, blogs, cameras, instant messaging, digital images and/or mobile phone technologies such as short messaging service (SMS). To harass, embarrass, threaten or hurt a person. This includes inappropriate communication via mobile devices, setting up a defamatory personal website or deliberately excluding someone from social networking spaces.

Cyberbullying can be pervasive and incessant. It differs from face-to-face bullying in that the bully may 'follow' their victim 24/7, and continue the bullying using technology at any time. Cyberbullies may take advantage of the perception of anonymity (e.g. using an account in a fake name, or a blocked number).

Cyberbullying can be particularly harmful as it is often a public form of humiliation and many others are able to see what is written or posted. Once messages/images are posted publicly online, it is very difficult to remove.

Its use can create a risk to another person's health or safety – either psychologically or physically – or their property, reputation, or social acceptance. It can cause hurt, self-harm or make someone fear for their safety.

Cyberbullying behaviours can include but are not limited to:

- Inappropriate verbal suggestions;
- Jokes or innuendo aimed at an individual to embarrass and humiliate:
- Sending inappropriate, insulting or threatening texts, picture messages, emails, or instant messages (e.g. Instagram, Snapchat or Facebook);

This document was reviewed and accepted by the Board of Governance of the Wyndham Community and Education Centre Inc on 07/12/17 and supersedes all previous versions.

Version: 2017 v1 Document number: 372 Page 2 of 6 G:\2017\2017 Compliance_P&P_AQTF\Policies\Access equity\cyber bullying.docx

- Sending/display of inappropriate images such as forwarding or sharing unflattering or private images without permission;
- Sending and/or forwarding sexually explicit images ('sexting'); People of any age, who forward or share images of a sexual nature of a person under 18 need to be aware that this is a criminal offence (child pornography) that may result in prosecution;
- Publishing someone's private, personal or embarrassing information without permission, or spreading rumors / lies online;
- Posting mean or nasty comments or pictures in chat forums;
- Offensive or inappropriate phone calls or SMS:
- Forwarding other's private emails, messages, pictures or videos without permission;
- Assuming someone's identity online and negatively representing them in a way that damages their reputation or relationships;
- Creating hate sites or implementing social exclusion campaigns on social networking sites;
- Applying inappropriate pressure to another person to speak or act in a particular way;
- Targeting another person with inappropriate words or actions;
- Name calling;
- Encouraging others to socially exclude someone / intentionally excluding others from an online group;
- Damaging someone's social reputation and social acceptance;
- Stealing passwords / Using a person's password to access their account and then pretending to be them;
- Sending cruel and threatening messages or material;
- Placing embarrassing photos of people on the web;
- Creating fake profiles that are mean or hurtful;
- Repeated prank phone calls such as repeated hang ups, anonymous or threatening phone calls; and / or,
- Using technology to run a multi-step campaign to bully another person. For example, setting another student up to be assaulted, video-recording their humiliation, posting the video-recording online and then sending the website address to others.
- Using technology in a way that intentionally encourages or causes someone fear for their safety or self-harm.

Cyberbullying vs bullying

While cyberbullying is similar to bullying in some ways, there are also differences.

Differences:

 Cyberbullying can be difficult to escape and is incredibly invasive. It is more likely to occur outside of times at Wyndham CEC, including at home, and can happen anywhere.

This document was reviewed and accepted by the Board of Governance of the Wyndham Community and Education Centre Inc on 07/12/17 and supersedes all previous versions.

Version: 2017 v1 Document number: 372 Page 3 of 6

- Cyberbullying can involve a large audience.
- Cyberbullying can involve harmful material being widely and rapidly shared to a large audience, for example, rumors and images can be posted on public forums or sent to many people at once. This material can also continue to be available and harmful long after the cyberbullying has ceased.
- Cyberbullies have a sense of anonymity
- Cyberbullying can provide the bully with a sense of relative anonymity and distance from the target, so there is a lack of immediate feedback or consequences.

Similarities:

- Power imbalance The power imbalance between the 'bully' and the 'target',
 the repetitive nature of the bullying behaviour and the intent to harm,
 humiliate, embarrass, ostracise, or isolate can occur in bullying and
 cyberbullying.
- Types of behavior Types of behaviour including spreading rumours and making threats or insults, can occur in bullying and cyberbullying.
- Reasons for behaving in a bullying way People often engage in cyberbullying for the same reasons they engage in bullying.

Cyber bullying can be a crime under the law when it involves:

- Using ICT devices such as the internet or a phone in a threatening, harassing or offensive way
- Threats
- Stalking (including messaging someone to self-harm or scare them)
- Accessing internet accounts without permission
- Defamation (spreading lies to intentionally hurt someone's reputation)
- Encouraging self-harm or for the person to fear for their safety

There are also stalking offences in each state and territory. Stalking involves a persistent course of conduct by a person against a victim, which intends to make them feel fearful, uncomfortable, offended or harassed. This conduct may occur online (for example, by email or on social networking sites) or via text message

In Victoria, it is illegal to stalk a person. Stalking occurs where a person intentionally and persistently intends to cause another person to feel fearful, uncomfortable, offended or harassed. This conduct may occur online (for example, by email or on social networking sites) or via text message.

Version: 2017 v1 Document number: 372 Page 4 of 6 G:\2017\2017 Compliance_P&P_AQTF\Policies\Access equity\cyber bullying.docx

Conduct that may be considered stalking is:

- telephoning or contacting someone electronically by email, chat rooms, SMS, or messenger, where the intention is to cause another to fear for their own safety or the safety of another or to cause another physical or psychological harm; or
- providing offensive material to another or leaving it to be found by a person (this would include posting offensive photos or messages via email, on networking pages such as Instagram, Snapchat, Google +, Facebook or You Tube or in chatrooms or message boards).

Using text messaging, emails or telephones, mobile phones, to make a threat or to harass or menace someone can also constitute a range of other crimes.

Where cyberbullying involves:

- comments that injure the personal and professional reputation of an individual; or
- exposing that person to ridicule or causing other people to avoid them, it may amount to defamation. A person who has been defamed may be able to sue the other person.

Responsibilities

Any student, client or employee who believes they have been a victim of cyberbullying is encouraged to inform the offender that their behaviour is unacceptable and against Wyndham CEC policy.

Any student, client or employee who has knowledge of cyberbullying occurring should inform a member of the Management team as soon as possible so that action can be taken.

Any victim of cyberbullying should seek the support of their Manager or the CEO as appropriate. Any behaviour that makes a person feel offended, threatened, scared, intimidated or uncomfortable is against Wyndham CEC policy and unlawful.

Procedure

All reports of cyberbullying should be treated seriously and thoroughly investigated by the relevant service unit Manager and / or the CEO if appropriate.

On completion of the investigation, the Manager in consultation with the CEO will determine the course of action to be taken.

The CEO will keep the Board informed of any investigation or actions undertaken.

Breaches of this policy will have consequences ranging from a written warning, counselling, dismissal, exit from a program and / or legal proceedings.

This document was reviewed and accepted by the Board of Governance of the Wyndham Community and Education Centre Inc on 07/12/17 and supersedes all previous versions.

Version: 2017 v1 Document number: 372 Page 5 of 6

It should be noted that incidents of offensive or suspicious online behaviour should be reported to the Australian Communications and Media Authority (ACMA) http://www.acma.gov.au/ or the Australian Federal Police depending on the nature of the behaviour.

Serious cyberbullying or stalking cases can also be reported to the Australian Cyber Crime Online Reporting Network (ACORN).

The Office of the Children's eSafety Commissioner protects Australian children when they experience cyberbullying by administering a complaints scheme and deals with complaints about prohibited online content. Contact details are: https://www.esafety.gov.au/complaints-and-reporting/offensive-and-illegal-content-complaints/report-offensive-or-illegal-content

Email: enquiries@esafety.gov.au

Tel: 1800 880 176

Where there is a reasonable belief that illegal activity or misuse of technology may have occurred, Wyndham CEC may report the suspected illegal activity or misuse of technology may lead to police involvement.

Note: See the Harassment, Discrimination, Victimisation and Bullying Policy & Procedure for more information regarding Bullying.

Version: 2017 v1 Document number: 372 Page 6 of 6 G:\2017\2017 Compliance_P&P_AQTF\Policies\Access equity\cyber bullying.docx