**Clontarf Beach State High School Cybersafety Policy**

Clontarf Beach State High Schoolembraces the opportunities that technology and the internet provide to students for learning, being creative and socialising online. Use of online communication and social media sites and apps can provide positive social development experiences through an opportunity to develop friendships and shape identities. When used safely, social media sites and apps can provide positive opportunities for social learning and development. However, inappropriate or misguided use can lead to negative outcomes for the user and others.

Clontarf Beach State High Schoolis committed to promoting the responsible and positive use of social media sites and apps. No student of Clontarf Beach State High Schoolwill face disciplinary action for simply having an account on Facebook or other social media site. As outlined on Pages 13 and 14 of the school’s Responsible Behaviour Plan for Students – Bullying and Cyberbullying, it is unacceptable for students to bully, harass or victimise another person whether within Clontarf Beach State High Schoolgrounds or while online.

Inappropriate online behaviours can have a negative impact on student learning and the good order and management of Clontarf Beach State High School– whether those behaviours occur during or outside school hours. This policy reflects the importance of students at Clontarf Beach State High Schoolengaging appropriately when online and is to be read in conjunction with the school’s Responsible Behaviour Plan for Students.

**Role of Social Media**

* The majority of young people use social media sites and apps on a daily basis for school work, entertainment and to keep in contact with friends. Unfortunately, some young people misuse social media technologies and engage in cyberbullying.
* Social media by its nature will result in the disclosure and sharing of personal information. By signing up for a social media account, users are providing their personal information.
* Students need to remember that the internet is a free space and many social media sites and apps have limited restrictions placed upon allowable content and regulated procedures for the removal of concerning posts.
* Social media sites and apps are designed to share online content widely and rapidly. Once students place information and/or pictures online, they have little to no control over how that content is used.
* The internet reaches a global audience. Even if students think that comments or photos have been deleted, there can be archived records of the material that will continue to be searchable into the future.
* Inappropriate online behaviour has the potential to embarrass and affect students, others and the school for years to come.

**Appropriate Use of Social Media**

* Students of Clontarf Beach State High Schoolare expected to engage in the appropriate use of social media if they choose to be online. Specific examples of appropriate use of social media sites and apps include:
* Ensure that personal information, such as full name, address, phone number, school name and location or anyone else’s personal information, is not shared.
* Think about what is posted online, and how it could be interpreted – avoid posting content that would be inappropriate to display in a crowded room, or in front of influential people. Once content is posted online, control is lost.
* Avoid provoking or engaging with another user who is displaying inappropriate or abusive behaviour. Rather than responding, address cyberbullying concerns using the online reporting tools, and seek support from an adult.
* If inappropriate online behaviour directly negatively impacts on the good order and management of Clontarf Beach State High Schoolthe school may impose disciplinary consequences for that behaviour regardless of whether the behaviour occurs during or outside of school hours.
* Disciplinary consequences could include suspension and/or exclusion. In serious cases of inappropriate online behaviour, the school may also make a report to the police for further investigation.
* Clontarf Beach State High Schoolwill not become involved in concerns of cyberbullying or inappropriate online behaviour where the incident in question does not directly negatively impact upon the good order and management of the school. For example, where cyberbullying occurs between a student of this school and a student of another school outside school hours. Such an incident will be a matter for parents and/or police to resolve.

**Laws and Consequences of Inappropriate Online Behaviour and Cyberbullying**

Inappropriate online behaviour may in certain circumstances constitute a criminal offence. Both the Criminal Code Act 1995 (Cth) and the Criminal Code Act 1899 (Qld) contain relevant provisions prohibiting types of online behaviour.

The Commonwealth Criminal Code outlines a number of criminal offences concerning telecommunications services. Potential relevant criminal offences are:

* using a carriage service to make a threat to kill or to cause serious harm to another person
* using a carriage service to menace, harass or cause offence to another person
* using a carriage service for child pornography material or child abuse material
* using a carriage service to promote methods for suicide or counsel another to commit

The Queensland Criminal Code contains several applicable sections for cyberbullying. Potential relevant criminal offences are:

* unlawful stalking
* computer hacking and misuse
* possession, distribution and making child exploitation material
* fraud - obtaining or dealing with identification information criminal defamation.

There are significant penalties for these offences.

Clontarf Beach State High Schoolstrives to create positive environments for all students at all times of the day, including while online. To help in achieving this goal, Clontarf Beach State High Schoolexpects its students to engage in positive behaviours while online.

**Incident Response Flow Chart**

1. **Initiate an Incident Response**

* Student, parent or carer reports cyberbullying incident to school. The report is referred to the student’s House Leader or House Dean
* Student to complete incident report, staff member to listen and record initial details into the cybersafety incident response plan (*By the end of the next school day*).
* The House Dean or House Leader will look at the facts and decide if the online behaviours negatively impact on the good order and management of the school.
* Inform other House Leaders or House Deans as required.
* Consider any external reporting requirements.

The Principal or Principal’s Delegate will firstly determine whether the incident negatively impacts on the good order and management of the school. This impact will need to be assessed at our school.

If the online behaviours *do not negatively impact on the good order and management of the school*, one of the following options should be considered:

* Inform parent/s of the students involved (and student if appropriate) that they may wish to consider reporting the online incident to an external agency such as QPS or Office of the eSafety Commissioner.
* Inform the parent/s of the option to report the online content/behaviour using the online tools provided by the website or app.
* Inform parent/s of the option to report the online content/behaviours through ACORN.
* The school leader may consider initiating contact with a law enforcement agency (LEA) by completing an LEA referral form.

This outcome and advice regarding further options should be made available to the parents using the Response Letter in Appendix 2.

If the online behaviours do negatively impact the good order and management of the school community continue to follow steps below:

1. **Gather and Preserve Evidence**

Gather and preserve any evidenceof inappropriate online behaviour or a potential unlawful online behaviour, where legally permissible. Record this into the cybersafety incident response plan.

|  |
| --- |
| **Note:** If the investigation involves sexting behaviours or child exploitation material, the school should respond in accordance with student protection procedures. |

When gathering evidence (except for naked or explicit images of children), do the following:

* Consider whether to confiscate mobile phones and other electronic equipment that may have been used in an incident. **Note:** confiscation can only be undertaken if in accordance with procedure Temporary removal of student property by school staff. Only Principal, Deputy Principal or SBPO can confiscate and/or take screen shots.
* Save emails and/or take screen shots of inappropriate content and save it in a secure location.
* Record the URL of the content if online or on social media
* Record any identifying particulars of the accounts involved, such as username, social media account, email, or mobile phone number
* Record the time, date and URL of any content captured.

**Is there a potential crime?** Appendix 3 lists potential criminal offences relevant to online behaviours and content.

**YES** If evidence of inappropriate behaviour or online activities that may be a potential crime is identified, this behaviour, depending on the crime, may eventuate in a criminal investigation. Principals may continue to investigate the matter for disciplinary purposes, subject to all laws and department procedures.

The school leader may consider initiating contact with an LEA by completing an LEA referral form. Police require the student be accompanied by a parent/s or the individual staff member affected by the online behaviour to make the official police complaint. A school leader cannot make an official complaint to police or via ACORN on behalf of a student or staff member.

**NO**

Content may not constitute a criminal offence, requiring involvement by police, but may nevertheless negatively impact the good order and management of the school. Principals may take action for this online behaviour in line with the school’s behaviour plan.

1. **Take Steps to Remove the Upsetting or Inappropriate Content**

It should be considered a priority to report and take steps to remove content which is viewable by a wider audience (such as on social media or a website) and is causing distress or affecting a staff member or student. Be mindful that not all content posted online is able to be removed and is dependent on the contents’ location on the internet or social media platform.

Options for removal:

1. The quickest method of removal is normally by requesting the person who posted the content to remove it. It should be explained to the student why the content is considered unacceptable.
2. Depending on the location of the content on the internet, some content is not able to be removed and will remain online permanently.
3. Online reporting through the website or app.
4. If assistance is required in removal of online content, contact the CSRM team on telephone 30345035 or email [Cybersafety.ReputationManagement@qed.qld.gov.au](mailto:Cybersafety.ReputationManagement@qed.qld.gov.au).

**Third-party Removal of Content**

If the student responsible refuses to delete the inappropriate or offensive content or if the identity of the person who posted the material is not known, then the principal, delegate, or victim will report the content to the service provider using their online reporting tools and request to have it removed. Most social networking providers have a ‘Report/Block this Person’ or ‘Report Abuse’ link on the content page or on the user’s profile.

Communications with third party providers should be limited to seeking removal of the content and stating how that content contravenes terms of service. It should be noted that some service providers (and in many cases, the police) do not accept reports by third parties, only allowing the account holder to make a request for assistance.

1. **Managing Student Behaviour**

Where the online behaviours of students have negatively impacted the good order and management of the school community, the Principal can take appropriate follow up action in accordance with the school’s Responsible Behaviour Plan for Students. Incident details and evidence recorded through the earlier incident management response steps may be used in formal decision making in accordance with departmental procedure (see the Safe, supportive and disciplined school environment procedure).

* Provide continued access to support for all involved.
* Set a timeline for any follow up and review.
* Ensure responsible officer continues to communicate with all parties.
* Provide information to parents and carers and escalation contacts if there is no satisfactory progress.

Identify ongoing issues and take appropriate action

1. **Recording the Incident on OneSchool**

If the incident was resolved at school level, details of the incident as reported to the school and investigated through the incident management process can be recorded in the student’s OneSchool behaviour records. The cybersafety incident response plan should be saved as an attachment.

**Note:** If the incident involves content which is naked or explicit images of children, do not save the image onto the OneSchool record. As an alternative, have two school leaders note descriptions of the image if there was a need to have actually viewed the image for the investigation.

**Cybersafety Incident Response Plan**

Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Year Level:\_\_\_\_\_\_\_\_\_\_\_\_\_

Care Class:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ House Dean:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Who was involved:

**Summary of Incident/ Evidence Collected:**

When gathering evidence (except for naked or explicit images of children), do the following:

* Consider whether to confiscate mobile phones and other electronic equipment that may have been used in an incident. **Note:** confiscation can only be undertaken if in accordance with procedure Temporary removal of student property by school staff. Only Principal, Deputy Principal or SBPO can confiscate and/or take screen shots.
* Save emails and/or take screen shots of inappropriate content and save it in a secure location.
* Record the URL of the content if online or on social media
* Record any identifying particulars of the accounts involved, such as username, social media account, email, or mobile phone number
* Record the time, date and URL of any content captured.

**School Actions/Possible Consequences**

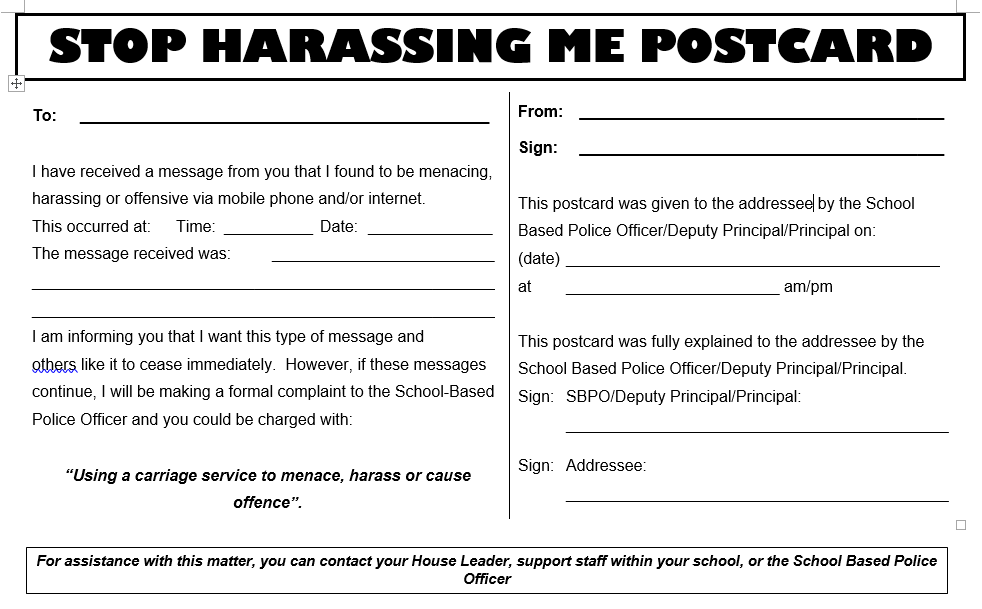
* Do the online behaviours negatively impact on the good order and management of the school? YES / NO
* If YES then continue to complete the response plan.

|  |  |
| --- | --- |
| Mean/Rude Behaviour | Cyber Bullying |
| * Behaviour discussion focusing on 4 Bs * Warning * Detention * Parent contact * Student is informed that the support team is available if they require any support * All students involved and/or parents are informed that if there are any ongoing issues or escalation then they should contact the student’s House Leader or House Dean immediately. | First reported instance:   * Behaviour discussion focusing on 4 Bs * Warning * Detention * Parent contact * Student is informed that the support team is available if they require any support * SBPO & Post Card Process (See appendix 1) * All students involved and/or parents are informed that if there are any ongoing issues or escalation then they should contact the student’s House Leader or House Dean immediately. |
| Subsequent issues:   * Explicit warning * Suspension * Referral to support team/ counselling | * Detention * Exclusion |

**Appendix 1 – SBPO & Post Card Process**



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



**Appendix 2 – Incident Response Letter for Non-School Issue**

Dear {Parent/Gaurdian}

{Student name} has reported an incident regarding cybersafety to the school on {Date}.

Clontarf Beach State High Schoolembraces the opportunities that technology and the internet provide to students for learning, being creative and socialising online. Use of online communication and social media sites and apps can provide positive social development experiences through an opportunity to develop friendships and shape identities.

When used safely, social media sites and apps can provide positive opportunities for social learning and development. However, inappropriate or misguided use can lead to negative outcomes for the user and others. Clontarf Beach State High Schoolis committed to promoting the responsible and positive use of social media sites and apps.

Clontarf Beach State High Schoolstrives to create positive environments for all students at all times of the day, including while online. To help in achieving this goal, Clontarf Beach State High Schoolexpects its students to engage in positive online behaviours.

The principal or principal’s delegate has investigated the incident. At present the school has determined that this issue, while upsetting, does not negatively impact on the good order and management of the school. We encourage yourself or {student name} to contact your student’s House Leader or House Dean if there are any further issues that take place in the future.

If you would like to pursue the issue outside of school one of the following options should be considered:

* Reporting the online incident to an external agency such as QPS or Office of the eSafety Commissioner.
* Report the online content/behaviour using the online tools provided by the website or app.
* Report the online content/behaviours through ACORN.

When gathering evidence (except for naked or explicit images of children), do the following:

* Save emails and/or take screen shots of inappropriate content and save it in a secure location.
* Record the URL of the content if online or on social media
* Record any identifying particulars of the accounts involved, such as username, social media account, email, or mobile phone number
* Record the time, date and URL of any content captured.

If you have any questions or would like to discuss the matter further then please don’t hesitate to call the school.

House Dean Principal

**Appendix 3 – Types of Inappropriate Online Behaviours on Social Media, Mobile Devices, and Electronic Technology**

Examples of social media and electronic communication technology incidents which may negatively impact on the good order and management of the school include:

* Creating imposter accounts of other students and teachers on social media apps, websites or online gaming platforms.

Student A creates a social media account in the name of Student B. Student A uses this account to impersonate Student B and send harassing messages to other students.

* Sexting: possessing, taking, distributing or posting nude or explicit images or video of another student, coercing or pressuring another student to take, distribute nude or explicit images or video of themselves.

Student A asks Student B to take a photo of themselves naked. Student B takes the photo and sends it to Student A. Student A then shares the image of Student B throughout the school.

Creating meme, gossip or hate pages about a school on social media apps or websites where the online presence is used to target students and staff members of that school.

A group of students create a social media account for other students of their school topost offensive and mean ‘gossip’ about other students.

Violent and dangerous videos: filming, sharing device-to-device or distributing online content, which involves students, involved in violent acts.

* Two students get into a fight during lunch time. A number of students film the fight and start sharing it on social media.

Dangerous or risky behaviours that involve choking, asphyxiation or other activities dangerous to a student’s health and wellbeing.

* Cyber abuse or cyberbullying: online behaviour that is reasonably likely to have a seriously threatening, intimidating, harassing or humiliating effect on a person. This behaviour may occur on various online spaces such as social media websites/apps, school email or online gaming platforms.

Student A posts a bullying comment on Student B’s photo they recently uploaded on social media. Student B deletes the comment but Student A continues to send harassing comments on social media directed at Student B.

* Taking photos or filming or voice recording a staff member or other student without consent and sharing the image or video online.

A group of students film their English teacher during class without consent. The students then share this video on social media and write harassing comments about the teacher who is in the video.

**Appendix 4 – Criminal Offences**

Cyberbullying and other forms of inappropriate online activity may in certain circumstances constitute a criminal offence. Both the Criminal Code Act 1995 (Cth) and the Criminal Code Act 1899 (Qld) contain relevant provisions.

Criminal Code Act 1995 (Cth)

The Criminal Code Act 1995 (Cth) Part 10.6 Division 474 of the Commonwealth Criminal Code outlines a number of criminal offences concerning telecommunications services when used with intent to commit a serious offence. Potentially relevant offences are:

* using a carriage service to make a threat to kill or to cause serious harm to another person (s.474.15)
* using a carriage service to menace, harass or cause offence to another person(s.474.17)
* using a carriage service for child pornography material (s.474.19)
* possessing, controlling, producing, supplying or obtaining child pornography material for use through a carriage service (s.474.20)
* using a carriage service for child abuse material (s.474.22)
* possessing, controlling, producing, supplying or obtaining child abuse material for use through a carriage service (s.474.23)
* using a carriage service to promote methods for suicide or counsel another to commit suicide (ss.474.29A and 474.29B).

Criminal Code Act 1899 (Qld)

The Queensland Criminal Code contains several applicable sections for cyberbullying and other online behaviours. Potential relevant offences are:

* unlawful stalking (s.359E)
* possession of child exploitation material (s.228D)
* involving a child in making child exploitation material and making child exploitationmaterial (ss.228A and 228B)
* distribution of child exploitation material (s.228C)
* criminal defamation (s.365)
* counselling, aiding or procuring suicide (s.311)
* obtaining or dealing with identification information (s.408D).

Criminal offences and definitions

Criminal Code Act 1995 (Cth) – current as of 5 March 2018

Under section 473.1 of the Criminal Code Act 1995 (Cth), “child pornography material” is defined as:

**“child pornography material”** means:

1. material that depicts a person, or a representation of a person, who is, or appears to be, under 18 years of age and who:

(i) is engaged in, or appears to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); or

(ii) is in the presence of a person who is engaged in, or appears to be engaged in, a sexual pose or sexual activity;

and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive; or

1. material the dominant characteristic of which is the depiction, for a sexual purpose, of:

(i) a sexual organ or the anal region of a person who is, or appears to be, under 18 years of age; or

(ii) a representation of such a sexual organ or anal region; or

(iii) the breasts, or a representation of the breasts, of a female person who is, or appears to be, under 18 years of age;

in a way that reasonable persons would regard as being, in all the circumstances, offensive; or

(c) material that describes a person who is, or is implied to be, under 18 years of age and who:

(i) is engaged in, or is implied to be engaged in, a sexual pose or sexual activity (whether or not in the presence of other persons); or

(ii) is in the presence of a person who is engaged in, or is implied to be engaged in, a sexual pose or sexual activity;

and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive; or

(d) material that describes:

(i) a sexual organ or the anal region of a person who is, or is implied to be, under 18 years of age; or

(ii) the breasts of a female person who is, or is implied to be, under 18 years of age;

and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive.

**child abuse material** means:

(a)material that depicts a person, or a representation of a person, who:

(i)is, or appears to be, under 18 years of age; and

(ii)is, or appears to be, a victim of torture, cruelty or physical abuse;

and does this in a way that reasonable persons would regard as being, in all circumstances, offensive; or

(b)material that describes a person who:

(i)is, or is implied to be, under 18 years of age; and

(ii)is, or is implied to be, a victim of torture, cruelty or physical abuse;

and does this in a way that reasonable persons would regard as being, in all the circumstances, offensive.

In Australia, under the Criminal Code Act 1995 (Cth) Part 10.6 Division 474 it is a criminal offence when:

* using a carriage service to access, transmit, make available, publish, distribute,advertise and solicit child pornography material (s.474.19)
* to have possession or control of material, produces, supplies or obtains material thatis child pornography material for use through a carriage service (s.474.20)
* using a carriage service to access, transmit, make available, publish, distribute,advertise and solicit child abuse material (s.474.22)
* to have possession or control of material, produces, supplies or obtains material thatis child abuse material for use through a carriage service (s.474.23).

The maximum penalty for the offences under s.474.19, s.474.20, s.474.22 and s.474.23 is 15 years imprisonment.

Criminal Code Act 1899 (Qld) – current as of 5 March 2018

The Criminal Code Act 1899 (Qld) section 207A, defines child exploitation material (CEM) as “material that, in a way, is likely to cause offence to a reasonable adult, describes or depicts a person, or a representation of a person, who is, or apparently is, **a child under 16 years—**

(a)in a sexual context, including for example, engaging in a sexual activity; or

(b)in an offensive or demeaning context; or

(c)being subjected to abuse, cruelty or torture.”

In Queensland, under the Criminal Code Act 1899 (Qld) it is a criminal offence when a person:

* involves a child in making child exploitation material (s.228A)
* makes child exploitation material (s.228B)
* distributing child exploitation material (s.229C)
* possesses child exploitation material (s.228D).

The maximum penalty for the offences under s.228A, s.228B, s.228C and s.228D is 20 years’ imprisonment and 25 years if the offender is using a hidden network or anonymising service. Possible inclusion on the Australian National Child Offender Register.

**Appendix 5 – Resources**

Further assistance

**Australian Cybercrime Online Reporting Network**

report.acorn.gov.au

**Office of the eSafety Commissioner**

[www.esafety.gov.au/complaints-and-reporting](http://www.esafety.gov.au/complaints-and-reporting)

Further information

**Bullying No Way!**

bullyingnoway.gov.au

**Headspace**

headspace.org.au/

**Kids Help Line**

kidshelp.com.au

**Meet the Creeps – Creep Quiz: Are U safe online? Queensland Government** creepquiz.eq.edu.au

**Queensland Police Service** police.qld.gov.au/programs/cscp/personalsafety/children/childprotection/

Think U Know, Australian Federal Police

thinkuknow.org.au

Social media training package

learningplace.eq.edu.au/Pages/default.aspx

(search ‘Introduction to social media management’ under staff space)

**Appendix 6 – Social Media Ages**

