Police response to cyberbullying and the Harmful Digital Communications Act

Table of Contents

Policy statement and principles

What

Using a mobile phone, the internet, or other technology such as a digital camera to hurt, harass, embarrass, threaten, blackmail, or intimidate somebody is cyberbullying and may also involve sextortion.

People of all ages use communication technology to bully and harass others and it encompasses, mobile to mobile, computer to mobile and vice versa and computer to computer. The various forums utilised include but are not limited to, instant messaging, voice over IP such as Skype, video posts such as You Tube and social media sites like Facebook and Twitter.

The Harmful Digital Communications Act 2015 is aimed at deterring, preventing and mitigating harm caused to individuals by digital communications; and providing victims of harmful digital communications with a quick and effective means of redress. The HDC Act achieves this by establishing both a civil and a criminal regime. The civil regime requires an Approved Agency - Netsafe - to assess, investigate and resolve complaints about harm caused by digital communications. The HDC Act also creates three criminal offences:

1. failing, without reasonable excuse, to comply with an order of the District Court pursuant to the Act; and
2. causing harm by posting a digital communication. The HDC Act also provides for applications to the District Court for certain orders and deals with the liability of online content hosts; and
3. posting intimate visual recording without consent (knowledge or reckless).

Why

Key goals of Police are preventing crime and victimisation, and targeting and catching offenders. There is also a growing body of evidence that links bullies to criminality and family violence. Enforcement of the Harmful Digital Communications Act 2015 maximises safety, addresses offending and its causes and reducing the harm caused to individuals in our communities.

How

Police will ensure that:

- the communication principles listed in the HDC Act (s6) are taken into account
- a multi-sector approach is taken with other agencies (e.g. NetSafe, Bullying-free NZ, Spark NZ, 2 Degrees and One NZ) to dealing with harmful digital communications
- every opportunity is taken to prevent harm caused by harmful digital communications
- victims of harmful digital communications seeking assistance are advised, supported and assisted with:
    - protection and, where appropriate, harmful digital communication orders
    - advice on where to obtain educational material and assistance from other agencies
- where:
    - any offences are identified, appropriate enforcement action is taken
    -
    no offence is disclosed, harm prevention action is taken.

Overview

Harmful Digital Communications Act 2015 and section 131AB Crimes Act 1961

The Harmful Digital Communications Act 2015 sets out communication principles and enforcement provisions relating to any form of electronic communication including any text message, writing, photograph, picture, recording or other matter that is communicated electronically.

The Act is intended to deter, prevent, and mitigate harm caused to individuals by digital communication (e.g. internet and mobile phone text bullying and harassment), and provide victims of harmful digital communication with a quick and efficient means of redress.

Section 131AB of the Crimes Act 1961 creates an offence that is targeted at persons 18 years or older using electronic communications such as social media platforms to harm persons under 16 ("young persons"). While the amendment focuses on online grooming practices, it covers all kinds of communications whether digital or not.

Seeking assistance against harmful digital communications

Advice and assistance with harmful digital communications can be obtained from:

- NetSafe - an independent non-profit organisation that promotes confident, safe, and responsible use of online technologies (**Note:** NetSafe is an approved agency under the Harmful Digital Communications Act 2015.)
- Police Cybercrime Unit as the Police Liaison with Netsafe
- these mobile phone providers:
    - Spark NZ
    - One NZ
    - 2 Degrees
- Police 'Kia Kaha' bullying prevention resources for schools and information for parents
- Internet content hosts, such as:
    - Facebook
    - WhatsApp
    - SnapChat (https://support.snapchat.com/co/harassment).

Related information

Further guidance is available from these sources:

- 2 Degrees
- Bullying Prevention Advisory Group
- Bullying prevention and response: A guide for schools
- Bullying-free NZ website
- Cyberbullying
- Digital Technology: Safe and responsible use in schools
- Education.govt.nz - Deter bullying: Promoting positive behaviour
- 'Hate crimes and hate incidents investigations' chapter for information about recognising, recording and dealing appropriately with **hate crime**, **hate incidents** and **hate speech** within the context of scene attendance, investigations, applying proportionality and using discretion
- NetSafe
- Online Safety Advisory Group
- 'Police response to bullying of children and young people' chapter
- Police 'Kia Kaha' bullying prevention resources for schools
- Preservation and recovery of electronic evidence chapter
- 'Social Networking, Open Source Information and Online Practitioner' chapter
- Spark NZ
- Transnational technology enabled crime - Advice to investigators

- One NZ

Health and safety duties for Police

Police employees responding to harmful digital communications complaints must be mindful of their following health and safety duties.

Maximising safety and minimising risk

Maximising safety and eliminating or minimising risk at work is the responsibility of all Police employees and persons engaged by Police to provide a service including contractors and their employees, trainees, interns and volunteers. It is delivered through meeting the obligations under the Health and Safety at Work Act 2015 and Police safety policies.

A key enabler is the application of the TENR-Operational threat assessment in the workplace.

The expectation of the Commissioner and the Act is that persons in the workplace will take reasonable care to ensure that their acts or omissions do not adversely affect the health and safety of other persons, comply as far as they are reasonably able to with any reasonable instruction that is given in order to comply with the Health and Safety at Work Act 2015 or regulations under that Act. They will co-operate with any reasonable policy or procedure relating to health or safety at the workplace that has been notified to them and take immediate action to stop any perceived or potential breach of the Act or if impractical, immediately report the matter to a supervisor.

Health and safety should be an everyday conversation

See 'Health, safety and wellbeing', 'Safer people' and this chapter in relation to the safe investigation of harmful digital communications and harassment complaints to ensure everyone is kept safe.

Definitions and principles under the Harmful Digital Communications Act 2015

This table provides hyperlinks to definitions of terms under section 4 of the Harmful Digital Communications Act 2015.

Term	Definition
Digital communication	Digital communication means: - any form of electronic communication; and - includes any text message, writing, photograph, picture, recording, or other matter that is communicated electronically.
Harm	Means serious emotional distress.
Individual	Individual means a natural person. **Note**: Companies, organisations etc. are not covered, but may still be liable under the Act.
Intimate visual recording	intimate visual recording means: - a visual recording (for example, a photograph, videotape, or digital image) that is made in any medium using any device with or without the knowledge or consent of the individual who is the subject of the recording, and that is of: - an individual who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and the individual is: - naked or has his or her genitals, pubic area, buttocks, or female breasts exposed, partially exposed, or clad solely in undergarments; or - engaged in an intimate sexual activity; or - engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing; or - an individual's naked or undergarment-clad genitals, pubic area, buttocks, or female breasts which is made: - from beneath or under an individual's clothing; or - through an individual's outer clothing in circumstances where it is unreasonable to do so; and - includes an intimate visual recording that is made and transmitted in real time without retention or storage in: - a physical form; or - an electronic form from which the recording is capable of being reproduced with or without the aid of any device or thing.
IPAP (internet protocol address provider)	IPAP has the same meaning as in section 122A(1) of the Copyright Act 1994: - IPAP, or Internet protocol address provider, means a person that operates a business that, other than as an incidental feature of its main business activities: - offers the transmission, routing, and providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing; and - allocates IP addresses to its account holders; and - charges its account holders for its services; and - is not primarily operated to cater for transient users.
Online content host	Online content host, in relation to a digital communication, means the person who has control over the part of the electronic retrieval system, such as a website or an online application, on which the communication is posted and accessible by the user.

Post	Post, in relation to a digital communication: - means to transfer, send, publish, disseminate, or otherwise communicate by means of a digital communication: - any information, whether truthful or untruthful, about the victim, or - an intimate visual recording of a victim an individual; and - includes an attempt to do anything referred to in the first bullet point paragraph above.
Victim	Victim means: - in relation to the offence of causing harm by posting digital communication (s22), an individual who is the target of a posted digital communication; and - in relation to the offence of posting intimate visual recording without consent (s22A), an individual who is the subject of an intimate visual recording.

Non-legislative definitions

Offline and online bullying or harassing behaviours are closely linked. Increasingly, people move seamlessly between offline and online environments, blending information and communications from different sources and media.

Bullying

The widely-accepted definition of bullying behaviour, as stated in 'Bullying prevention and response: A guide for schools', emphasises the following four characteristics:

- bullying is deliberate
- bullying involves a power imbalance
- bullying has an element of repetition
- bullying is harmful.

Cyberbullying

Cyberbullying is bullying that is enabled, enhanced, or in some way mediated through digital technology (e.g. email, mobile phones, chat rooms, social networking sites and instant messaging). See also 'Cyberbullying characteristics'.

Communication principles

This table provides communication principles under section 6 of the Harmful Digital Communications Act 2015.

Principles	A digital communication should not:
Principle 1	disclose sensitive personal facts about an individual.
Principle 2	be threatening, intimidating, or menacing.
Principle 3	be grossly offensive to a reasonable person in the position of the affected individual.
Principle 4	be indecent or obscene.
Principle 5	be used to harass an individual.
Principle 6	make a false allegation.
Principle 7	contain a matter that is published in breach of confidence.
Principle 8	incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.
Principle 9	incite or encourage an individual to commit suicide.
Principle 10	denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.

Note: Police employees performing investigations and exercising powers under the Act must:

- take account of these communication principles
- act consistently with the rights and freedoms contained in the New Zealand Bill of Rights Act 1990.

Cyberbullying characteristics

Bullying using technology (cyberbullying) can be more complex and harder to deal with than traditional physical bullying, because it:

- enables a person to attack someone online and still remain anonymous. This and better access to (or ability to use) technology creates an imbalance of power regardless of age, physical strength or social status
- can involve people who have never met in real life and who have no social connections.

Cyberbullying has fewer boundaries than physical bullying. This is because digital information can be:

- quickly shared, spread and viewed
- stored in multiple locations
- created and shared automatically
- stored in a way that only certain groups can see
- shared and posted at any time of the day or night
- left as a permanent record (e.g., photos posted on the internet).

See Cyberbullying page on 'Bullying Free NZ' internet site for further information.

Sextortion

What is happening

Law enforcement globally is seeing an increase in reports of people being blackmailed online for financial gain. This involves offenders approaching victims on social media and tricking them into sending sexually explicit content before blackmailing them.

This is also known as Sexual Extortion or Sextortion and often includes threats to share the content with friends and family unless the victim pays money to the offender.

New Zealand is affected by the global trend of increased reports of younger, more vulnerable victims being targeted by offshore offenders.

The issue of online blackmail or sexual extortion against young people online is not new. However, it was previously rare to see this type of blackmail for money. Blackmail involves a threat to disclose something about a person, intending to cause harm or benefit from the accusation. See the 'Blackmail' chapter for further information.

Overseas organised criminal groups

Organised criminal groups operating from overseas are targeting young people and it is likely the vast majority of New Zealanders are victims of these groups. s.6(c) OIA

How offenders operate

s.6(c) OIA, s.6(d) OIA

Taking a report or complaint

This table outlines the taking of a report or complaint of sextortion.

Step	Action
1	Code instances of sextortion as blackmail pursuant to Section 237 of the Crimes Act 1961. **Note:** The correct NIA Precedent Code is 1748.
2	s.6(c) OIA

Initial Action: What you need to do

Initial action is similar for cases involving adult and young persons as victims. This table outlines the initial action you need to take.

Step	Action
1	Note, OCEANZ may be able to offer specialised advice for those cases involving young people.
2	Reassure the victim that they have done the right thing in reporting the matter to Police. **No blame should be placed on the victim**.
3	Obtain a formal written statement from the victim, and include: s.6(c) OIA
4	s.6(c) OIA
5	Obtain a victim impact statement from the victim (POL392).
6	s.6(c) OIA
7	Complete a victim support referral. Go to Police Forms > Victims > Victim Support Referral .
8	s.6(c) OIA

s.6(c) OIA

s.6(c) OIA

Orders related to harmful digital communications

The purpose of harmful digital communications orders is to deter, prevent and mitigate harm caused to individuals by digital communications.

Applications for orders

Certain listed individuals may make applications for Court orders under section 18 (interim) and 19 (full) of the Act (s11) where there complaint has firstly been considered by Netsafe and they are not satisfied with the outcome (s12). Police may also make such an application if the digital communication constitutes a threat to the safety of an individual. Police are not required to have the matter firstly considered by Netsafe. Applications must be filed in the District Court (s15).

Click on this link to obtain an application form.

Orders that may be made by District Court

Orders that may be made by the District Court are covered by sections 19, 20 and 22B of the Harmful Digital Communications Act 2015.

Against defendant

The District Court may, on an application, make one or more of the following orders against a defendant under section 19:

- an order to take down or disable material
- an order that the defendant cease or refrain from the conduct concerned
- an order that the defendant not encourage any other persons to engage in similar communications towards the affected individual
- an order that a correction be published
- an order that a right of reply be given to the affected individual
- an order that an apology be published.

Against online content host

The District Court may, on an application, make one or more of the following orders against an online content host:

- an order to take down or disable public access to material that has been posted or sent
- an order that the identity of the author of an anonymous or pseudonymous communication be released to the court
- an order that a correction be published in any manner that the court specifies in the order
- an order that a right of reply be given to the affected individual in any manner that the court specifies in the order.

Against an internet protocol address provider (IPAP)

The District Court may, on application, make an order against an IPAP that the identity of an anonymous communicator be released to the court.

Court may make additional directions

The District Court may also do one or more of the following:

- make a direction applying an order provided for against a defendant or against an online content host to other persons specified in the direction, if there is evidence that those others have been encouraged to engage in harmful digital communications towards the affected individual
- make a declaration that a communication breaches a communication principle
- order that the names of any specified parties be suppressed.

Matters for Court to take into account with making order

In deciding whether or not to make an order, and the form of an order, the court must take into account the following:

- the content of the communication and the level of harm caused or likely to be caused by it
- the purpose of the communicator, in particular whether the communication was intended to cause harm
- the occasion, context, and subject matter of the communication

- the extent to which the communication has spread beyond the original parties to the communication
- the age and vulnerability of the affected individual
- the truth or falsity of the statement
- whether the communication is in the public interest
- the conduct of the defendant, including any attempt by the defendant to minimise the harm caused
- the conduct of the affected individual or complainant
- the technical and operational practicalities, and the costs, of an order
- the appropriate individual or other person who should be subject to the order.

Note: The court must act consistently with the rights and freedoms contained in the New Zealand Bill of Rights Act 1990.

The Court may vary or discharge an order made under section 18 or 19 (s20).

Court may make civil order during proceedings for posting intimate visual recording without consent offence under s 22A

On application and if the court considers it desirable to do so, the court conducting the proceedings for an offence under section 22A may make:

- during the proceedings, 1 or more of the interim orders set out in the 'Interim orders' paragraph below against the defendant for the duration of the proceedings; and
- if the defendant is proven to have committed the offence 1 or more of the orders set out against the defendant below.

Interim orders

The following interim orders are available to the court during the proceedings:

- an order to take down or disable material
- an order that the defendant cease or refrain from the conduct concerned
- an order that the defendant not encourage any other persons to engage in similar communications towards the affected individual.

Orders available to court when defendant proven to have committed offence

The following orders are available to the court when the defendant is proven to have committed the offence:

- an order to take down or disable material
- an order that the defendant cease or refrain from the conduct concerned
- an order that the defendant not encourage any other persons to engage in similar communications towards the affected individual
- an order that a correction be published
- an order that a right of reply be given to the affected individual
- an order that an apology be published.

Where a defendant is proven to have committed an offence

A defendant is proven to have committed an offence under section 22A if:

- the defendant is convicted of the offence; or
- the defendant is found guilty of, or pleads guilty to, the offence, but is discharged without conviction under section 106 of the Sentencing Act 2002; or
- the Youth Court makes an order under section 282 of the Oranga Tamariki Act 1989 discharging the charge relating to the offence after finding that the offence was proved.

Multi-sector approach to dealing with harmful digital communications

Multi-national initiative

Police, the Internet Safety Group (NetSafe - for internet providers/applications e.g. Facebook and Twitter), telecommunication providers and other agencies from the education, health, justice, social and human rights sectors, have agreed to work together and offer advice to:

- reduce the incidence of harmful digital communications
- reduce victimisation
- identify offenders
- take measures that include:
    - community education
    - early intervention
    - the identification and prosecution of persistent and/or serious offenders.

Bullying Prevention Advisory Group

Bullying Prevention Advisory Group (BPAG) is a collaboration of 18 organisations, with representatives from the education, health, justice and social sectors, as well as internet safety and human rights advocacy groups.

BPAG members share the strongly held view that bullying behaviour of any kind is unacceptable and are committed to ensuring combined action is taken to reduce bullying in New Zealand schools.

Online Safety Advisory Group

The Online Safety Advisory Group (OSAG) is a subgroup of the multi-agency Bullying Prevention Advisory Group (BPAG), which advises the Ministry of Education's programme for schools to manage challenges related to bullying. OSAG not only considers issues specifically related to cyberbullying, but also broader online safety issues that challenge schools, and how they plan for and manage online safety. OSAG has produced the publication 'Digital Technology: Safe and responsible use in schools'.

Bullying-free NZ

Bullying-free NZ provides information to agencies, schools, students, parents and whanäu and embodies a philosophy that "together with a shared vision, we know which direction to go, together - we can prevent bullying in Aotearoa".

Educational material

NZ Police

The Police 'Kia Kaha' bullying prevention resources for schools and information for parents to address issues of bullying and harmful digital communications.

Online content hosts

Online content hosts provide educational material, such as:

- Facebook
- WhatsApp
- SnapChat (https://support.snapchat.com/co/harassment).

Spark, One NZ and 2 Degrees

Spark, One NZ and 2 Degrees publish educational material on mobile phone safety, including steps that can be taken to reduce the likelihood of being a victim of cyberbullying and options available if it does occur. This information is publicly available from their respective Internet sites. See the section 'Seeking assistance against harmful digital communication' in this chapter.

NetSafe

Educational information on text and cyber bullying is also available from NetSafe and from the NetSafe Freephone text and cyber bullying helpline on 0508 NETSAFE (0508 638 723).

NetSafe

Netsafe's role

Netsafe has been appointed as the Approved Agency under the Harmful Digital Communications Act (HDCA) 2015 to manage complaints about digital communications which may have caused, or are likely to cause, harm to a person.

Netsafe's role is to negotiate with the relevant parties to achieve a satisfactory outcome. This may include working with online content hosts to take down material and facilitating agreements between parties to cease harmful digital communications (HDC).

Anyone has the right to apply to the District Court for civil orders but before doing so they must have engaged with the Approved Agency process. They can apply regardless of whether Netsafe has taken actions under section 19 of the HDCA.

The victim, a parent/guardian, a school leader as well as the Police and the Chief Coroner may all apply to the District Court under the HDCA.

Netsafe can:

- investigate complaints where harm has been caused and attempt to reach settlements
- contact producers of harmful digital communications and request that they:
    - remove/edit communications
    - desist from communicating
- liaise with website hosts, internet service providers (ISPs) and other internet intermediaries (both here and overseas) and request them to take down or moderate posts that are clearly offensive
- refer victims to Police for section 22 and 22A offences
- inform people about their legal options and the possible outcome if they wish to proceed to the District Court (civil orders).

Netsafe cannot:

- use search, surveillance and seizure powers - such as those typically given to law enforcement agencies. Netsafe can only access content that is publicly available online and work with the evidence supplied
- punish people for their actions online, or force them to take action such as removing content.

Netsafe's process for dealing with HDC complaints

This table outlines the NetSafe process for dealing with complaints.

Stage	Description
1	Receive complaints via a number of channels: - webform - email - social media - phone.
2	Consider whether the reporter of the complaint is valid. **Note:** Under section 11 the report must come from: - the affected individual or: - a parent/ guardian of the individual - the professional leader of a registered school or his/ her delegate - the Police if the communications constitutes a threat to safety of the individual.

3	Clarify if the complaint constitutes a serious breach of any of the ten communication principles by assessing evidence to determine if one or more of ten communication principles may have been seriously breached. See 'Communication principles' for the list of principles.
4	Decide whether the case passed the threshold for 'harm'. Under section 11 of the Act the affected individual must have suffered or will suffer harm. 'Harm' is defined as serious emotional distress. The HDCA lists factors that may be used to determine whether a communication would cause harm, including: - the extremity of the language used - the age and characteristics of the victim - whether the digital communication was anonymous - whether the digital communication was repeated - the extent of circulation of the digital communication - whether the digital communication is true or false - the context in which the digital communication appeared.
5	Attempt to achieve a successful resolution between parties. Under section 8 of the Act Netsafe can use persuasion, negotiation, mediation and advice to try to attempt to find a resolution. Resolution options may include but are not limited to the following: - provide education and advice on online safety and conduct - advise people on steps they can take to resolve a problem (social media tools / security features) - liaise with website hosts, ISPs and other internet intermediaries (both here and overseas) and request them to take down or moderate posts that are clearly offensive - liaise with Enforcement partners - this may include Police/ DIA who may have information on active investigations related to the same case - contact producers of harmful digital communications and attempt to mediate - refer victims to Police for section 22 and 22A offences.
6	Provide a 'complaint summary' if the victim wishes to proceed to the District Court. Regardless of the outcomes that Netsafe does or does not achieve, everyone has the right to apply to the District Court for a civil order. To do this they require a 'complaint summary' from Netsafe that gives high level information. For example, communication principle(s) Netsafe considered the case against, names of the victim and the 'producer'. **Notes:** - At this point the Netsafe process effectively stops. Netsafe do not help people fill in application forms and are not involved in the Court process. - Should the District Court find that there has been a breach of the HDCA, the Court may make order(s)against the defendant, against online content host and against an internet protocol address provider (IPAP). - Netsafe should be informed by the Court registrars of decisions made under section 19 of the HDCA.

Netsafe contact details

Email: queries@netsafe.org.nz

Phone: 0508 NETSAFE (0508 638 723).

Spark, 2 Degrees and One NZ process

Spark's Call Investigation Centre, 2 Degrees Service Centre and One NZ's Customer Care team respond to thousands of customer inquiries each month regarding unwanted calls and texts. A very small number are serious enough to advise the caller to go to Police. As per agreed guidelines, all complaints referred to Police on the advice of Telecom or One NZ must be investigated.

Spark, 2 Degrees and One NZ attempt to resolve complaints on behalf of customers with the aim of preventing further complaints. Action can include sending a warning message to the initiator of the text and barring that person from using the handset on the network. It is up to the Telco to decide what action they will take and the Police cannot make any promises to the complainant about what action the Telco might take.

When a Telco classifies the content as serious enough to refer on to Police, the customer is advised to personally contact Police and take their mobile phone with them. The customer is also advised to collate any examples for showing to Police.

The general customer inquiry number relating to mobile phone support is 0800 800 163 for Spark, 0800 022 022 for 2 Degrees and 0800 800 021 for One NZ.

When do Police become involved?

Offences

This table details the offences that could apply.

Offence and offence code	Penalty
Non-compliance with (harmful digital communication) order (1765) Section 21 Harmful Digital Communications Act 2015 Person without reasonable excuse, fails to comply with an order made under section 18, 19 or 22B.	Natural person: 6 months imprisonment or fine not exceeding $5,000 Body corporate: fine not exceeding $20,000
Causing harm by posting digital communication (1766) Section 22 Harmful Digital Communications Act 2015 Person: - posts a digital communication with intention that it cause harm to a victim; and - posting the communication would cause harm to an ordinary reasonable person in the position of the victim; and - posting the communication causes harm to the victim. Determining whether post would cause harm, the Court may take into account any factors it considers relevant, including - the extremity of the language used - the age and characteristics of the victim - whether the digital communication was anonymous - whether the digital communication was repeated - the extent of circulation of the digital communication - whether the digital communication is true or false - the context in which the digital communication appeared. **Notes:** - Section 22 does not apply if the posted digital communication is an intimate visual recording to which the offence in section 22A (posting intimate visual recording without consent) applies. - Harm is defined to mean “serious emotional distress”. **Must prove:** There was an intention of causing harm to the person who is the subject of the posting.	Natural person: 2 years imprisonment or fine not exceeding $50,000 Body corporate: fine not exceeding $200,000

Posting intimate visual recording without consent (1767) Section 22A Harmful Digital Communications Act 2015 There are two offences under section 22A: - Posting intimate visual recording without consent (knowledge) - Posting intimate visual recording without consent (reckless). **Offence ingredients** Person, without reasonable excuse, posts a digital communication that is an intimate visual recording of a victim: - knowing that the victim has not consented to the posting;**or** - being reckless as to whether the victim has consented to the posting. **Notes:** - An individual under the age of 16 years cannot consent to the posting of an intimate visual recording of which they are the subject. - No requirement to prove an intention of causing harm to the person who is the subject of the posting.	Natural person: 2 years imprisonment or fine not exceeding $50,000 Body corporate: fine not exceeding $200,000

Grooming for sexual conduct with young person (2744) Section 131AB of the Crimes Act 1961 **Offence ingredients** A person aged 18 years or over: - communicates by words or conduct with a person under the age of 16 years (the**young person**), **and** - they do so, intending to facilitate the young person engaging or being involved in conduct that would be against: - any of the other Part 7 of the Crimes Act offences, these offences include: - indecent act in a public place (section 125) - sexual violation (section 128B) - sexual conduct with young person under 16 (section 134) - indecent assault (section 135), **or** - section 98AA(1)(a)(i), (d)(i), (e)(i), or (f)(i) of the Crimes Act. These offences all relate to the sexual exploitation of young people. A "young person" under section 131AB can also be a constable pretending to be a young person. Where the communicator believes the fictitious young person is a real person under 16 years of age, they will be liable under section 131AB. It does not matter whether the young person responds to the communication. **Defences for the section 131AB offence** Section 131AB(4) contains a defence to the offence. A person who is charged under section 131AB will have a defence where they can prove that: - before the time they took the action concerned, they had taken reasonable steps to find out whether the young person was of or over the age of 16 years; and - at the time they took the action concerned, they believed on reasonable grounds that the young person was of or over the age of 16 years. Taking 'reasonable steps' will not require the person charged to do everything possible to ascertain the recipient's age. It will merely require them to take any steps a reasonable person would think sensible to ensure the recipient is 16 years or older. The steps taken should provide information reasonably capable of supporting a belief that the recipient is of legal age, which might call for more diligent inquiries in some circumstances compared to others. Where the communication takes place online, for example, it can be hard to tell whether a person is honestly representing themselves. Therefore, more steps might be required of someone initiating digital communications.	A person aged 18 years or over is liable to imprisonment for a term not exceeding 3 years.
Intimidation Section 21(1)(a) - Summary Offences Act 1981	3 months imprisonment or a fine not exceeding $2,000.
Criminal harassment Section 8 - Harassment Act 1997	2 years imprisonment.
Contravening a protection order Section 49 - Domestic Violence Act 1995	2 years imprisonment.

Misuse of a telephone device Section 112 - Telecommunications Act 2001	3 months imprisonment or a fine not exceeding $2,000.
Aiding and abetting suicide (incites, counsels or procures another person to commit suicide) Section 179 - Crimes Act 1961 **Note:** Offence committed even if that person does not commit or attempt suicide in consequence of that conduct.	3 years imprisonment.
Wounding with intent Section 188 - Crimes Act 1961 (From New Zealand case law (*R v Mwai*) it appears likely that psychiatric injury (expert evidence) caused by menacing text messages could amount to bodily harm in terms of section 188)	14 years imprisonment.
Meeting young person under 16 following sexual grooming, etc. Section 131B - Crimes Act 1961	7 years imprisonment.

Note: If it is felt that the texts received are part of a grooming offence (section 131B above), the CIB or Child Protection Team should be consulted at the time of taking the complaint. For the incident to be a grooming offence the victim must be under sixteen years of age and therefore the correct point of contact is the Child Protection Team.

More information on grooming offences can be found in the 'Child protection - Mass allegations and online offending against children' chapter.

No offence disclosed: then prevent harm

Even if no offence has been identified, this may still provide an opportunity to prevent harm (as per Prevention First 2017). For schools in particular, there is a process to follow for any report of bullying (including cyber), whether or not an offence is disclosed.

See: the 'Police Response to Bullying of Children and Young People' chapter for further guidance.

Consider advising the person to contact their mobile service provider or online contents host and seek their specific assistance. See the section 'Seeking assistance against harmful digital communication' in this chapter for links to the service providers.

If the situation is complicated, involves schools or workplaces, or young people, the NetSafe Contact Centre (0508 NETSAFE - 0508 638 723) can offer additional advice and information, including advice on cyber bullying.

Receiving and investigating complaints/reports

Procedure for receiving complaints/reports

Follow these steps (not necessarily in order) when you receive a complaint/report of harmful digital communications.

Step	Action
1	Ascertain the complaint relates to causing harm by posting digital communication, posting intimate visual recording without consent, threatening, harassing, sexually offensive or other seriously disturbing content, or non-compliance with (harmful digital communication) order. If not sure, discuss with NetSafe. **Remember** that Netsafe may be having content removed online that could form part of your evidence. **Note:** - Do **not** disregard the victim. If clearly **not** a Police issue refer appropriately. - All reports of harmful digital communication involving children or young people be recorded in NIA with the **6P incident code** (bullying of children and young people) and if offending is identified, an offence code must be added. - If complaint involves adults and offending is identified, an offence code must be recorded in NIA.
2	If complaint or report of harmful digital communication involves children or young people take the following actions: - record in NIA with the **6P incident code** - if offending is identified, an offence code must be added - discuss a range of prevention activities that: - are based on the cross-sector publication 'Bullying prevention and response: A guide for schools' - may include the nine components of the whole school approach described in the Police's school wide intervention plans - provide advice and support to the victim, initiator, parents/caregivers to prevent future bullying behaviour: - advice based on the bullying pamphlets for young people and for parents and caregivers available from the Kia Kaha section on the School Portal - support as required (e.g. referral to appropriate agency). See 'Procedure when bullying is reported' in the 'Police response to bullying of children and young people' chapter for further information.
3	If complaint or report involves adults and offending is identified, an offence code must be recorded in NIA.
4	Complete case management process for: - recording incident, offence - initial attendance (see also 'Procedure when bullying is reported' in the 'Police response to bullying of children and young people' chapter for additional steps to be undertaken for school-based bullying) - process forensics.
5	Record: - full particulars of victim (customer) and note demeanour - particulars of mobile phone including phone number, brand, model number and serial number (if any and visible) to identify the handset. If the phone is turned on, enter *#06# on the phone keypad. In most instances this will give you the handset serial number or International Mobile Equipment Number (IMEI) number. - date and time narrative of events in sequence including what if any incident may have caused the harassment to start.
6	Ask complainant: - to display or play any collated messages or PXT/videos - for any known particulars of suspect, including mobile phone number and reason for suspicion.

7	Consider capturing any digital evidence. This may involve your local Digital First Responder (DFR) or Digital Forensic Unit (DFU). As a minimum, take a digital photograph of any text: - with time and date stamp and then make a transcription or record messages if possible with time and date stamp - that has been sent in reply along with time and date stamp. Then make a transcription of any message reply the complainant may have made or times when a voice reply has been made.
8	Advise the victim: - to retain messages on handset for evidential purposes (depending on seriousness of messages and capacity of handset) - not to respond to any further messages - to keep the time, date and content of any further messages from the same number or same caller and save any threatening or sexually explicit messages on their handset - consider personal support available including school counsellor, family members, victim support agencies - that NetSafe on Freephone 0508 NETSAFE (0508 638 723) can provide additional advice and information.
9	In some circumstances a harmful digital communications order may be advisable. Discuss with your local Prosecution section.
10	Issue a Complaint Acknowledgement Form.

Procedure for investigating complaints/reports

Follow these steps when you investigate a complaint/report of harmful digital communications.

Step	Action
1	Check procedural steps for receiving a complaint/report of harmful digital communications have been completed and the case management process for: - recording incident, offence - initial attendance (see also 'Procedure when bullying is reported' in the 'Police response to bullying of children and young people' chapter for additional steps to be undertaken for school-based bullying) - process forensics.
2	Assess, screen and link case (case management process).
3	Prioritise case (case management process).
4	Investigate case (case management process), including: - obtain information using information request form/production order from the relevant: - telecommunication service provider - online content host.
5	If using information request form (IRF): **Go to** Police Forms (I-Z) > Information Requests Production Orders > Information Request Form / Production Order Cover Sheet (wait 3 seconds and 'Information Request Form - Page 1' information box will appear on the screen) > complete details in the box. **Note:** Once the form has been completed it must be approved by an authorised approver from the currentlypublished list, this can be either by physically signing the IRF or by the approver forwarding it to the service provider by email.
6	If obtaining a production order, see 'Application procedure for production orders' in 'Production Orders' of the 'Search' chapter.
7	Where offending is identified and the victim is under the age of 18 at the time of making the complaint, the'Child protection investigation policy and procedures' apply and must be complied with. This includes ensuring that any appropriate notifications are made to Ministry for Vulnerable Children (Oranga Tamariki). Employees are encouraged to take advice from Child Protection Teams in respect of serious cases and in particular those where sexual offending is alleged.

Procedure for resolution, proceedings and case disposal

Resolution, proceedings and case disposal action is to comply with the case management process. If offending is identified and the victim is of or under the age of 18 years at the time of making the complaint the 'Child protection investigation policy and procedures' apply and must also be complied with.

At the conclusion of the investigation, advise the complainant and the relevant telecommunications provider or online content host of the result.

Note: The agreed processes for each provider are confidential between the individual provider and Police. Do not disclose the process by which Police obtain information from complainants, other telecommunication providers or online content hosts.