

# THE REP: INTERNET

This education kit will help you facilitate a conversation with young people about their legal rights online and when using technology. It includes classroom activities, workshop slides and background legal notes. This workshop is designed to last between 1-1.5 hours.





# How to deliver a REP module

*Use this information to inform your facilitation.*

Kia ora! Thank you for being a REP volunteer. Your participation in The REP will help young Aotearoaians become more aware of their legal rights and responsibilities. By connecting young people with local support services, you will also help build a stronger community for all of us. So... what do you need to know about delivering a module?

## Know your Community Law Centre

- The most important thing about The REP is the connection you can build between members of your community and your local Community Law Centre.
- If a class takes only one thing out of a workshop, it should be that if they have a legal problem they can get help from their local Community Law Centre or YouthLaw.
- Use The REP modules as a way of talking about how Community Law Centres, other community-based services and lawyers can actually help. Learn about local support services available for youth in your area.
- If anyone in your class asks for help or needs legal advice (which you are not allowed to give if you are not a lawyer), direct them to their local Community Law Centre.
- Consider going the extra step: go along with a student to a Community Law Centre so they feel supported.

## Know the audience

- The second most important thing about The REP is that our education is meant to be interactive and fun. Getting your audience to relax and have a laugh is as important, if not more important, than talking about the law.

- Treat this resource as a guide only – try hard to deliver the material in a way that will suit your audience and that your audience will enjoy.
- REP modules are learner-led, so focus on what the class wants to talk about. There is no need to cover all the material in the time you have been given. See where the conversation goes, focus on what the class identifies as being important or relevant, and explore those ideas. Just to repeat: there is no need to get through all the material!

## THE REP: INTERNET

Opening	5
Icebreaker	6
<b>SECTION 1</b>	
Online bullying, harassment and online abuse	7
<b>SECTION 2</b>	
Staying safe online	11
<b>SECTION 3</b>	
Harmful Digital Communications	15
<b>SECTION 4</b>	
Online privacy	20
Closing	23

Copyright © Community Law Wellington and Hutt Valley 2019  
info@wclc.org.nz

- Every group you work with will be different, with different levels of knowledge, different needs, and different expectations. Let the group both guide and teach you; work together to build a picture of how the law actually works in New Zealand.
- Try and get to the heart of the matter: talk about the real world, and the greater social implications of the law. You will get much more out of it, and so will your class.

### *Know the activities*

- In general, everybody likes to know why they are here, whether it's relevant, and how long it will take. Take your time to signpost what the module is going to cover and the activities, by explaining or perhaps writing up a short plan on the board.
- These modules are structured so that all the important information can be covered through running the activities. The activities aim to get your class thinking about the issues being discussed and engage with them in a practical way.
- It is important to know and understand the way the activities are run, so you can lead them smoothly and effectively.
- If you can think of more diverse, more engaging and more fun games and exercises, please do. Just make sure you feed these new improved activities to us at The REP.

### *Know the law*

- You need to be up-to-date with the area of law this module covers.
- That said, you are not expected to know everything! If you don't know an answer, a good technique is to reflect the question to the whole class or say you will find out and let them know. Remember, if you say you will find something out, make sure you do.
- The background material in this guide is to help you learn the law. The Community Law Manual is also a fantastic guide to all the areas of 'community' law. Check out the manual online for the relevant chapters to this module here: [www.communitylaw.org.nz](http://www.communitylaw.org.nz).
- It's always helpful to have some relevant examples up your sleeve of how the law works in practice. If in doubt, check out the news, talk to your friends, family, teachers, or the lawyers and other kaimahi at your local Community Law Centre.



### *Know some different teaching styles*

- Everybody learns differently. Very few people enjoy being lectured to!
- The activities in this module attempt to cater for different kinds of learners:
  - Some people like to visualise what they're learning (by seeing it written down, making a list or studying an image)
  - Other people need to hear things to take them in (maybe by listening to a story or using rhythm or sound as memory aids)
  - Some people learn by talking (by sharing with a neighbour or taking part in a discussion)
  - Other people prefer to learn while moving around (when up on their feet and active)
  - And others learn with their hands (getting creative, drawing or cutting things out)
- Work hard at improving your own facilitation practice so that everybody can get involved in the class.

### *From the outset, it is important to*

- Establish a safe space. Be aware that the modules contain sensitive content. The key is how you leave the young people *feeling*, so make sure class members are comfortable at all times.
  - For example, if a young person blushes when answering a question, say "have a think about it" and move on to someone else or if a joke is made about a class member, divert the heat onto yourself
  - If you notice that a young person seems triggered, approach them quietly and one-on-one or flag it with their teacher
- Build rapport with the young people. Be respectful, honest and authentic. Young people have a lot of lived experience, so start with the assumption that they know more than you. If you give them the chance to step up, they will.
- Establish flexibility. There is no 'right' way to facilitate these modules. If the class is only interested in one topic, that's fine. Be responsive to your audiences' needs and their body language.
  - For example, if the energy is flat, mix the games up and start with an activity involving movement or with a pair exercise "talk to your neighbour about..."
- Make participation voluntary. Encourage everyone to be involved, but always ask for volunteers so no one is embarrassed by being singled out. Don't ask the young people to do anything you wouldn't do!



- Work with the teacher. Most classes are likely to have a teacher present during your session so check in before the class starts. If something disruptive happens, ask the teacher to step in.
- Have fun! If you're having fun, the class will have fun. Having funny anecdotes helps the class relate to the content and if the session is fun and interesting, young people are more likely to remember.

### ***Evaluations***

- Getting feedback is essential to improving The REP. Leave enough time at the end of the class to hand out and collect the evaluation forms. And remember to feed this back to us at The REP.
- Don't forget to fill in your facilitation evaluation form!

### ***Last, but not least...***

... Smile! Enjoy yourself, have a laugh, and thanks again for volunteering your time.

## **WHAT YOU WILL NEED**

- Projector and laptop
- Slides (Ctrl+L for fullscreen)
- Facilitator notes
- Printing materials
  - Activity #1: 1 × set per class (cut out before)
  - Activity #2: 1 × per pair
  - Activity #3: 1 × set per class
  - Activity #4: 1 × A3 per group
- Blu Tack
- Evaluations 1 × per class member
- Chocolate
- Community Law Centre flyers

## **Student safety**

This module contains sensitive content. It's crucial that all participants feel safe during this session. Make sure you begin by explaining to the class that taking time out is okay. Let them know that if something comes up during the session they can speak to their teacher, school counsellor, someone they trust, their local Community Law Centre or YouthLaw. Talk to a teacher before the class starts to find out what support is available to students if required.

# Opening



## THE REP: THE INTERNET

 **REP.**  
RIGHTS EDUCATION PROJECT

 **CL**

### GREETINGS

- “Kia ora, talofa lava, ni hao, hello” (introduce yourself, your name, a bit about yourself).
- “This session is brought to you by the Community Law Centre and The REP: the Rights Education Project”.
- Introduce the Community Law Centre:
  - Community Law Centres provide free legal advice, on most topics. You can see a lawyer, for free, on anything to do with employment, family, criminal, tenancy, debt, and beyond
  - Make sure the class knows where to find their local Community Law Centre and how to contact YouthLaw. For example: “Your nearest Community Law Centre is in Wellington Central at 203 Willis Street on Level 8 or in Lower Hutt at 59 Queens Drive on Level 2. Come in and see us some time!” and “You can call YouthLaw on **0800 UTHLAW (0800 884 529)** to talk to someone who can help!”
  - Community Law Centres are situated throughout New Zealand and you can locate your nearest one at: [www.communitylaw.org.nz/our-law-centres/](http://www.communitylaw.org.nz/our-law-centres/)
- Introduce The REP:
  - We are here to let you know your legal rights and responsibilities. We present the law on a number of areas, but if you have anything you are particularly interested in, we are always open to new ideas!



## INSTRUCTIONS

- Talk to a teacher before the class starts to find out what support is available to students if required.  
.....
- The idea of this icebreaker is to encourage participation and to introduce the class members. Work hard to remember the names of everyone in the class.
- This icebreaker introduces the REP: Internet module by asking the class to say their name and answer a question.
- Ask the class “What is your favourite emoji (and why)?”
- Start off by introducing your favourite emoji. For example, the girl in the red dress (I’m a dancing queen) or the unicorn emoji (unicorns are my favourite animal).  
.....
- Before you start the next section make sure you say something like:
  - “Today we’re going to look at some difficult issues that many young people in Aotearoa experience. We’re going to talk about online bullying and what the law says. This problem affects one in three young people so we’re going to talk about those initiating bullying behaviour and those targeted by bullying behaviour, and what you can do to keep yourself and others safe.
  - It is very important that everyone feels safe during this session, so taking time out is okay. If something comes up for you during the session, speak to your teacher, school counsellor, someone you trust, your local Community Law Centre or YouthLaw.”

## SECTION 1

# Online bullying, harassment and online abuse

---



## RISKY BUSINESS

### ACTIVITY #1 INSTRUCTIONS

- Divide the class into four groups and give each group a 'Risky business' scenario card.
- Give the class some time to talk about the questions on the back of their card.
- Ask each group to read their scenario and facilitate a group discussion using the questions on the back of the scenario cards:
  - Could someone use this to hurt me or could it hurt someone else?
  - Would I be upset if this was shared with others?
  - What's the worst that could happen if I shared this?
- Reward good contributions to the discussion with chocolate!

## ACTIVITY #1

# Risky business

---

### Scenario #1

You get sent a dick pic from a boy in your class. He messages you again asking for a nude.

- It can be upsetting to receive a nude or sexual message that you didn't want or ask for.
  - It is always your choice whether you send a nude, so if you feel uncomfortable talk to someone you trust. Once you press send, it is nearly impossible to control what happens to your photos or videos.
  - Remember that if you send a nude that includes your face, it makes you much easier to identify you if it gets forwarded on.
- .....

### Scenario #2

You videoed a fight that your mate Jono was involved in with students from another school.

- Online bullying is bullying that takes place online or uses digital technology to send or publish content with the intention to harm someone.
  - Digital content can instantly be shared, spread and viewed by a wide audience and can be difficult to delete or remove.
- .....

### Scenario #3

Your friend sets up a group chat with all the girls in your class to talk about Miranda, who she says is a slut because she flirted with her boyfriend. She tells you on the group chat to back her up and send Miranda a message calling her out.

- Sending mean messages to someone is online bullying. Repeated messages to the point of harassment are also online bullying.
  - Even though it's just one comment, you could be a part of something much bigger that could cause serious harm.
- .....

### Scenario #4

You have your Facebook profile set to public. Your account is set up under your full name and your birthday, phone number and email address are on your profile.

- Approximately eight out of ten young people have an online profile that is visible to the public. Personal information shared online can be used to identify you and where you live, target you with online scams or steal or use your data or identity.
- So it's really important to protect yourself by not sharing your personal information online or on social media! For example, your home address, phone number and date of birth.



## LEGAL NOTES

*Learn this information and integrate it into your facilitation. Don't read it out word for word!*

### Online bullying

- Online bullying is bullying that takes place online or uses digital technology to send or publish content with the intention to harm someone.
- In Aotearoa NZ, one in three 10-24 year olds report having been cyberbullied (Behind the Screen report 2016).
- Access to technology means that it can happen at any time so people experiencing online bullying can be targeted 24/7.
- Digital content can instantly be shared, spread and viewed by a wide audience and can be difficult to delete or remove.
- Being able to remain anonymous and cyberbully someone creates an imbalance of power that doesn't depend on age, physical strength or social status. This means that even if someone wouldn't bully someone else in person, it is easier to say something online anonymously.
- Online bullying can happen to anyone and can be done by one person or a group (for example, members of an online community). The online bullying could be private (for example, a text message) or be more public (for example, a post on Facebook).
- Online bullying can include:
  - Sending mean texts, emails or messaging (for example, calling someone names or making fun of someone in a chat that includes multiple people)
  - Being shamed or called names online
  - Sending threatening texts, emails or instant messages
  - Posting hurtful messages, images or videos on social media (for example, posting an embarrassing video on Instagram)
  - Threatening to post sensitive or intimate photos or information online
  - Spreading lies, rumours or gossip about someone online (for example, anonymous messages or polls for example, on Tellonym)
  - Spreading private information about someone online
  - Pretending to be someone online by hacking their account
  - Creating a fake profile to make fun of you
  - Repeatedly attacking or killing an avatar or character in an online game

- Purposefully excluding people from online groups, chats or events
- Repeated and unwanted texts, calls or messages to the point of harassment
- The worst kinds of harassment – including online bullying – can be a criminal offence.
- There are a number of different laws that deal with online harassment. Some of them, like the Harassment Act, deal with harassment, bullying and intimidation regardless of the form of the behaviour – that is, whether it's face to face, or through a note in your letterbox, or through texts, emails and online posts.
- See the REP: Sex for more on protection from harassment.

### The harm from online bullying

- Online bullying can impact a whole school or kura community dramatically.
- Schools and kura are legally responsible for the emotional and physical safety of students. The responsibility extends to behaviour that occurs off-site if it affects a student's learning and wellbeing.
- Those targeted by online bullying can experience:
  - Missing or leaving school or kura
  - Impact on learning (seeing marks drop) or failure
  - Depression and anxiety
  - Low self-esteem
  - Self-harm and suicide
  - Detrimental effects on health and wellbeing
- Those who initiate online bullying are also affected:
  - Damage to your reputation
  - Criminal conviction which impacts on things like getting a job, travelling, housing – it could follow you for life
  - Maintaining positive relationships with your friends and family
  - Leaving school or kura early
- Bystanders
  - Online bullying also has a negative impact on those who witness bullying
  - Students say that seeing bullying in their school or kura makes them feel worried and uncomfortable

## ***Sending nudes***

- Nudes are when people send or receive sexual images or videos (for example, underwear shots or sexual videos) using apps on a phone or other electronic device. It can also include sexual text messages or chats.
- According to a Netsafe report, in the past 12 months:
  - One in five teens have been sent a nude they didn't ask for
  - One in five teens have been asked for a nude
- It can be upsetting to receive a nude or sexual message that you didn't want or ask for (for example, a dick pic). You can report the content or block the person from sending more pictures. It is also important to talk to someone you trust. See the next sections for more information on what you can do in this situation.
- It can also be distressing if you are asked for a nude but don't want to send one. It is always your choice whether you send a nude, so if you feel uncomfortable talk to someone you trust.
- Even if you agreed to a photo or video being taken (or took it yourself and sent it) that doesn't mean you consent to it being on-shared.
- But once you press send, it is nearly impossible to control what happens to your photos or videos.
- Remember that if you send a nude that includes your face, it makes you much easier to identify you if it gets forwarded on.
- If you have sent something you now regret, try to have an honest conversation with the person you sent it to as quickly as possible and ask them to delete it. This can help stop your information from being sent on later.
- Teens who send nude or sexual images are risking their image being forwarded on and could be breaking the law.

## ***Image-based sexual abuse***

- It is very important to think about the risks of sharing a nude or nearly nude image or video (for example, in your underwear) before you hit send.
- One big risk with sharing nudes is that these are shared with others, for example, if a relationship breaks up, or if friends have a fight. Once you send a message or image, it is impossible to control who sees it and very, very difficult to get back.

- Just because you consent to sharing with one person doesn't mean you consented to it being shared with others.
- Even on apps like Snapchat where messages disappear, people can still take a screenshot without you knowing and re-post it on another website.
- Sharing (or threatening to send) nudes or sexual images or videos with a wider group or publicly, without consent is an offence.
- Many criminal prosecutions under the Harmful Digital Communications Act are for image-based sexual abuse, for example:
  - A 16 year old female sent an intimate video to an older man and was blackmailed into sending more or else he threatened to release the original
  - A man sent a sex video of his partner to her mum
  - A woman found a sex video and a nude photo of herself on a porn website that her ex-partner had posted after they broke up
- Remember: If someone shares nude images of you without your consent it is never your fault and it's important to get support.
- Even if someone has altered a photo to make it look like an intimate image of you, this is still image-based abuse.
- See the next sections for what you can do in this situation.

## ***Before you share online ...***

- Ask yourself:
  - Could someone use this to hurt me?
  - Would I be upset if this was shared with others?
  - What's the worst that could happen if I shared this?
- Think about different perspectives and how people may react to a post or message:
  - Could it hurt someone else?
  - What would happen if your employer saw it?
  - Could someone use it against you?
- Remember that everything you post online stays online and can go much further than your original post.
- Never post something online about someone online that is untrue.

## SECTION 2

# Staying safe online

---



### ACTIVITY #2 INSTRUCTIONS

- Divide the class into pairs and give each pair a 'What now?' worksheet.
- Give the pairs time to complete the next steps in each scenario. Ask for ideas of all the different things you could do.
- Reward good contributions to the discussion with chocolate!

## ACTIVITY #2

# What now?

### Scenario #1

One of your friends uploads a photo to Instagram of you in your undies. They had taken it when they walked in on you getting changed at a sleepover. You thought it was a joke and they weren't going to do anything with it, but you feel really embarrassed. What can you do?

- **Ask them to stop:** If it's safe, try talking to the person privately about what they've said or done, and ask them to take down the post.
- **Talk to a trusted adult:** If your friend doesn't do what you asked, talk to an adult to discuss how you should deal with the situation.
- **Keep evidence:** Save texts/emails, record profiles/usernames of the people responsible and take screenshots/save URLs of online posts (keep track of dates, what has happened, who you think did it and why in case you need to forward to Netsafe or police).
- **Report it:** Look for a 'Report Abuse' button to complain to the online host or a 'Safety' link to access safety centres with tips on how to deal with bullying (you can also ask Netsafe to make a complaint for you or give you advice to make your complaint).
- **Contact Netsafe:** Netsafe can provide information, advice and support.

### Scenario #2

Someone sends you an anonymous message through an app "I guess the secret is out!" with a link to a page. The link takes you to a page someone has made about you. There are lots of comments from different people discussing rumours about all the boys you've been getting with. It has been going on for weeks. You feel humiliated and depressed as a result of the discovery. What can you do?

- **Don't reply:** Especially to messages from phone numbers, profiles or people you don't know.
- **Don't attack the person back:** Avoid giving them the satisfaction of a reaction.
- **Keep evidence:** Save texts/emails, record profiles/usernames of the people responsible and take screenshots/save URLs of online posts (keep track of dates, what has happened, who you think did it and why in case you need to forward to Netsafe or police).
- **Contact Netsafe:** Netsafe have experience dealing with these situations and may be able to find out who is using the Tumblr and request the content to be taken down.
- **Reach out:** The most important thing to do if you become a target online is to tell someone you can trust, for example, a whānau member or a close friend (it is important to talk to a trusted adult as they'll be removed from the situation and able to help you).
- **Call a support service:** If you would rather talk to someone else or you need some more support, there are lots of different services you can access (see below for contact details).
- **Change your username:** You could change your username or make a new profile.



## LEGAL NOTES

*Learn this information and integrate it into your facilitation. Don't read it out word for word!*

### What can you do?

- If you are experiencing online bullying, online harassment or abuse, there are a number of things you can do straight away to keep yourself safe:
  - **Don't reply:** Especially to messages from phone numbers, profiles or people you don't know
  - **Don't attack the person back:** Avoid giving them the satisfaction of a reaction
  - **Ask them to stop:** If it's safe, try talking to the person privately about what they've said or done
  - **Keep evidence:** Save texts/emails, record profiles/ usernames of the people responsible and take screenshots/save URLs of online posts as they may disappear later (keep track of dates, what has happened, who you think did it and why in case you need to forward to Netsafe or police)
  - **Block a phone number:** Some devices allow you to block numbers in the phone's settings otherwise you can report repeated unwanted calls or messages to your mobile phone provider (for example, for Spark call \*123 to block a caller or call the Calls Investigation Centre on 0800 809 806 or for Vodafone send BLACKLIST ADD followed by the number of the person you want to block to 713)
  - **Block/unfriend/unfollow:** Look for the 'block sender/user' button where you can manage a list of people you want to avoid, or unfriend/unfollow them (you could also mute their posts)
  - **Report it:** Look for a 'Report Abuse' button to complain to the online host or a 'Safety' link to access safety centres with tips on how to deal with bullying (you can also ask Netsafe to make a complaint for you or give you advice to make your complaint)
  - **Adjust your privacy settings:** Make sure you know your privacy settings (see the next section on online privacy)
  - **Change your username:** You could change your username or make a new profile

### Who can you contact?

- There are also things you can do to keep yourself supported and help deal with the situation:
  - **Reach out:** The most important thing to do if you become a target online is to tell someone you can trust, for example, a whānau member or a close

friend (it is important to talk to a trusted adult as they'll be removed from the situation and able to help you)

- **Call a support service:** If you would rather talk to someone else or you need some more support, there are lots of different services you can access (see below for contact details)
- **Tell a teacher if the person bullying you is another student at your school or kura:** Schools and kura have obligations to prevent online bullying if it relates to your participation at school or kura (for example, the person who is being targeted and the person who is initiating the bullying attend school or kura together, if the bullying is happening at school or kura, or on social media such as a class Facebook page)
- **Visit your local Community Law Centre or contact YouthLaw:** Speak to a lawyer for free who can explain your options. It's always a good idea to get advice before making a complaint!
- **Contact Netsafe:** If you need help or support with online bullying, harassment or abuse (see below for contact details)
- **Contact the police:** If you are receiving messages or posts involving threats to your safety contact your local police station (if you receive a threat about your immediate safety call 111)

### Where can you go for help?

- Learn about local support services so you have the best information about options for youth in your area.
- ICON is a web tool developed by Sticks n' Stones to help explore and deal with online negativity (with information and practical tips about nudes, online bullying, online abuse and staying safe online):
  - Website: [www.icon.org.nz](http://www.icon.org.nz)
- Youthline is a free 24/7 helpline for youth:
  - Phone: 0800 376 633
  - Free TXT 234 (between 8am-midnight)
  - Website: [www.youthline.co.nz](http://www.youthline.co.nz)
- WHAT'S UP is a free counselling helpline (12pm-11pm) and webchat service (3pm-10pm) for children and teenagers:
  - Phone: 0800 WHAT'S UP (0800 942 8787)
  - Website: [www.whatsup.co.nz](http://www.whatsup.co.nz)

- Rainbow Youth provides support for gay young people and their families:
  - Phone: (09) 376 4155
  - Website: [www.rainbowyouth.org.nz](http://www.rainbowyouth.org.nz)
- Lifeline is a free and confidential support helpline, available 24/7 and staffed by qualified counsellors:
  - Phone: 0800 LIFELINE (543 354)
  - Free TXT 'HELP' to 4357
  - Suicide Crisis Phone: 0508 TAUTOKO (828 865)
- Call the sexual harm helpline 'Safe to Talk' for 24/7 free information and support:
  - Phone: 0800 044344
  - Free TXT: 4334
  - Website: [www.safetotalk.nz](http://www.safetotalk.nz)
- The Depression helpline offers 24/7 access to counsellors who can help you find the right support:
  - Phone: 0800 111 757
  - Free TXT 4202
- Contact Netsafe seven days a week for advice and support:
  - Using their online form at [www.netsafe.org.nz/report](http://www.netsafe.org.nz/report) (or click on 'Report Online Incidents' on their homepage)
  - Email: [help@netsafe.org.nz](mailto:help@netsafe.org.nz)
  - Free phone: 0508 NETSAFE (638 723)
  - TXT 'Netsafe' to 4282
  - If you are concerned about your or someone else's immediate safety call 111

## SECTION 3

# Harmful Digital Communications



### ACTIVITY #3 INSTRUCTIONS

- Divide the class into groups and hand out a 'Pick a path' card to each group.
- Explain that sometimes the consequences of online behaviour can now become criminal. The Harmful Digital Communications Act makes online bullying, online harassment and image-based sexual abuse a criminal offence!
- Read out the scenarios below and tell each group to holds up their card(s) and explains why it is a good option in the situation.
- Reward good contributions with chocolate!

## ACTIVITY #3

# Pick a path

### Scenario #1

"Mandy meets an older guy at a party and is offered \$1000 to send a nude photo with her face in it. She decides the money would be worth it so she can buy those concert tickets! Mandy sends the video through and receives the money. The next day, she gets another message telling her to send him another nude video or he will send it to her school, family and friends..."

This is really serious. A harmful digital communication could be a criminal offence if:

- You suffered harm
- The person responsible meant to cause you harm
- Most people would agree the material was harmful or offensive

*Who should Mandy go to?*

- Contact Netsafe
  - Call the police
  - Talk to a trusted adult
  - Call a support service
  - Complain to the District Court
  - Contact YouthLaw or visit your local Community Law Centre
- .....

### Scenario #2

"Jenny and Hamish have been together for a year and a half when Jenny breaks up with Hamish. He is really upset when she tells him she is seeing someone else. He remembers that a few months ago they made a sex video for fun. He has suspicions that she was cheating on him so decides to upload the video onto Pornhub."

This is really serious. Many criminal prosecutions under the Harmful Digital Communications Act are for revenge porn incidents.

*Who should Jenny go to?*

- Contact Netsafe
  - Call the police
  - Talk to a trusted adult
  - Call a support service
  - Complain to the District Court
  - Contact YouthLaw or visit your local Community Law Centre
- .....

*continued...*



### *Scenario #3*

"Esther is one of the coolest girls in school. She uploads a photo on Instagram of Janey sitting by herself eating her lunch. There are heaps of comments and someone posts #likethispostifyouthinkjaneyshouldkillherself". One of Janey's friends tag her in the post so she sees what is happening. "

This is really serious. It is criminal offence to encourage someone to commit suicide (even if they do not attempt to take their own life). If convicted, the penalty is up to three years in prison.

#### *Who should Janey go to?*

- Contact Netsafe
- Call the police
- Talk to a trusted adult
- Call a support service
- Tell your school
- Complain to the District Court
- Contact YouthLaw or visit your local Community Law Centre

## LEGAL NOTES

*Learn this information and integrate it into your facilitation. Don't read it out word for word!*

### **Harmful digital communications**

- A law called the Harmful Digital Communications Act 2015 makes online bullying a criminal offence.
- A harmful digital communication could be a criminal offence if:
  - You suffered emotional or physical harm
  - The person responsible meant to cause you harm
  - Most people would agree the material was harmful or offensive (what the "reasonable person" would think)
- What is 'harmful' under the Harmful Digital Communications Act can take a variety of forms, including online bullying, online harassment, and image-based sexual abuse, for example:
  - Sending or publishing offensive or invasive messages, photos or videos
  - Sending or publishing personal information about another person
  - Threatening to share nude photos or videos
  - Spreading damaging or degrading rumours
  - Sending or publishing indecent photos
  - Harassing or intimidating people
  - Encouraging people to send messages to others to harm them
  - Encouraging someone to commit suicide, even if they don't attempt to take their own life
  - Sending or publishing degrading things about someone because of their colour, race, ethnicity, nationality, religion, gender, sexual orientation or disability
  - Blackmailing someone using intimate photos or videos
- 'Digital communications' can occur on a range of platforms including: Social media (for example, Instagram, Facebook, Messenger, Snapchat, Tumblr, Twitter, Tinder/Grindr) websites, apps, email, text messages, gaming platforms, blogs and forums.
- The law now explains ten Communication Principles that should guide online behaviour. Digital communications should never:
  - Share your personal information
  - Threaten you
  - Be offensive
  - Be indecent or obscene
  - Be used to harass you

- Make false allegations
- Share confidential information
- Encourage anyone to send harmful messages
- Encourage someone to commit suicide
- Speak badly about someone's colour, race, ethnicity, religion, gender, sexual orientation or disability

### **Contact Netsafe**

- Netsafe is an organisation that is responsible for online safety in Aotearoa NZ.
- Netsafe provides a free service to help keep people safe online.
- If you are harmed by online content (including online bullying and harassment) you can contact Netsafe for advice.
- Netsafe can:
  - Take reports of harmful digital communications
  - Give advice and discuss options to stop the online abuse, including the right to apply to the District Court for orders under the Harmful Digital Communications Act
  - Investigate complaints and try to come to an agreement between the targeted person and the person who published the content
  - Contact the person responsible for the communications to try and resolve the issue
  - Request website hosts and ISPs to take down or moderate harmful content
- You can report to Netsafe by:
  - Using their online form at [www.report.netsafe.org.nz/hc/en-au/requests/new](http://www.report.netsafe.org.nz/hc/en-au/requests/new) (or click on 'Report Online Incidents' on their homepage)
  - Email: [help@netsafe.org.nz](mailto:help@netsafe.org.nz)
  - Free phone: 0508 NETSAFE (638 723)
  - Txt 'Netsafe' to 4282
  - If you are concerned about your or someone else's immediate safety call 111

### **Report it to the online host**

- If you complain to the host about harmful online content (either on your own or through Netsafe) there are steps they need to take to protect themselves from legal responsibility:

- Send a copy of your complaint to the responsible person within 48 hours
- If they can't contact that person or the person doesn't respond, they must remove the post within 48 hours of your complaint being made
- The person responsible has 48 hours to respond and say if they agree to the material being removed or not
- If the person agrees, they must remove it asap
- If the person doesn't agree, you will need to contact NetSafe (see above) or complain to the District Court.
- If the host does not consider that the content breaches their community standards, it may not be taken down.

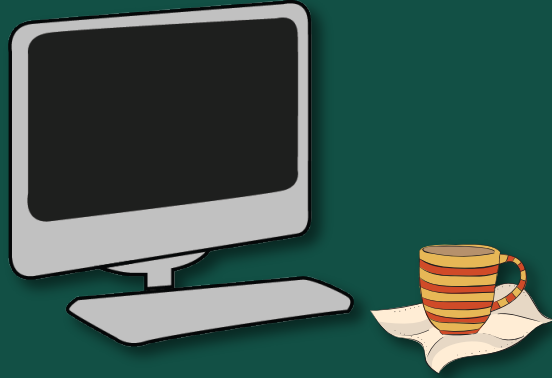
## ***Complaining to the District Court***

- If you have tried to resolve the issue through Netsafe first, the court may be able to fix the problem.
- You can complain to the court if you have suffered serious emotional distress because of online material (that is covered by one or more of the 10 Communication Principles outlined in the law), and the person meant to cause you harm.
- The court may make orders if there has been a serious breach (or threatend serious breach) of the Communication Principles.
- You, your parents/guardians, a school or kura representative (with your permission) or the police (if your safety has been threatened) can make the application for a Harmful Digital Communication order, for example, to:
  - Take down content
  - Stop a behaviour
  - Publish an apology or correction
- Give you a right of reply
- Release the identity of a person behind an anonymous communication
- Not encourage others to act in a similar way towards you
- Name suppression
- If someone is convicted of not complying with an order, the maximum penalty is up to six months in prison or a fine up to \$5000.
- It is a criminal offence to send messages and post material online that intend to cause serious harm. The maximum penalty is up to two years in prison or \$50,000 fine.
  - For example, an 18 year old who threatened to send naked pictures of his 16 year old ex-girlfriend to her mother was convicted and sentenced to 11 months in prison.
- If you are under 17 years old and commit an offence, the consequences may include:
  - A police warning
  - Attending a Family Group Conference (to address the behaviour)
  - Diversion (see the REP: Police)
  - Being taken to Youth Court (see the REP: Police)
  - The offending going on your criminal record (see the REP: Police)
- If you are over 17 years old and commit an offence, you will be treated as an adult by the court.
- It is also a serious criminal offence to encourage someone to commit suicide (even if they do not attempt to take their own life). If convicted, the penalty is up to three years in prison.

## SECTION 4

# Online privacy

## LOGO SKETCH



### ACTIVITY #4 INSTRUCTIONS

- Divide the class into groups and hand out a “Logosketch” worksheet to each group. The instructions are on the sheet.
  - Sketch the logos of as many social media apps as you can think of!
  - Pick one and come up with your Top Privacy Tip for that app
- Tell the class that each group will have two minutes to draw as many social media logos as they can think of - no looking at your phone!
- The group who comes up with the most logos wins chocolate!
- Ask each group to pick one of the apps they have drawn and come up with their ‘Top Privacy Tip’ for their favourite app.
- Facilitate a group discussion around why it is important to protect your privacy online.
  - Do you have Instagram, FB, Twitter, Snapchat?
  - Do you know your privacy settings?
  - Who has really good privacy settings?
  - When was the last time you checked?





## LEGAL NOTES

*Learn this information and integrate it into your facilitation. Don't read it out word for word!*

### Privacy laws in Aotearoa NZ

- There are laws in NZ that protect your privacy and how your personal information is used.
- These rules apply to most organisations, such as the board of trustees at your school or kura. For example, your old school or kura can't give your new school or kura your personal information without your permission and you have the right to know what your school or kura has told another school or kura about you.
- Your personal information means things that can identify you as an individual and includes:
  - Your name
  - Your address
  - A photo of your face
  - Employment details
  - Health information
- There is a Privacy Commission which upholds the privacy principles, for example, agencies must keep your information secure, must let you see your information if you ask and only collect information they lawfully and reasonably need.

### Keep online information private

- You have a very important role in keeping your information safe.
- Approximately eight out of ten young people have an online profile that is visible to the public.
- Personal information shared online can be used to:
  - Identify you and where you live
  - Target you with online scams
  - Steal or use your identity
  - Track your online activity
  - Steal your data
- So it's really important to protect yourself by not sharing your personal information online or on social media. This includes:
  - Your home address
  - Phone number
  - Date of birth
  - Email address
  - Full name
  - Age

- Once information is disclosed online, it can be hard to get it removed.
- Treat posting messages and uploading photos as if you are publishing your information publicly.

### Privacy safety tips

- Be aware that information you post privately could always be reposted and seen by people you didn't expect – even things you share with your friends can end up being shared publicly.
- Search yourself on Google to see what information is already out there.
- Before you post, think about people who might see your content in the future for example, employers, schools or kura, university or family members.
- Often default privacy settings for new social media accounts are public, so make sure to check this. If your account is public, bots can trawl your account for your personal information.
- Check your social media settings often to make sure you have an appropriate level of privacy on your posts.
- Only add people you know and trust to your social media followers or friends, so you are aware who is seeing your day-to-day status updates and photos. Use categories such as 'only friends' to limit who can see your information.
- Have a quick read through the privacy terms and conditions before you sign up to new apps or websites.
- Check with your friends and family before posting information or photos about them.
- Be aware that people may not be who they say they are online (catfishing) and make a safety plan if, for example, you agree to meet someone from Tinder irl.
- Delete anonymous feedback/polling platforms for example, Tellonym.
- Create different passwords that are hard to guess and never share them.
- Logout of your account before exiting the browser on shared computers.
- Use Secure Browsing whenever possible.

### Privacy settings

- Facebook:
  - The average number of Facebook friends is 338 – that's a lot of people who can see what you post!

- Change your 'Privacy Settings' to limit who sees your photos and posts to 'friends', 'friends of friends', 'only you' or a custom audience (if your account is public, bots can crawl your account for your personal information)
- Click on 'Privacy Shortcuts' to do a privacy checkup – choose who can search for you using your cellphone number/email address, who can add you as a friend and who can see your birthday or birth year
- The 'View As' tool to see your Facebook profile from the perspective of someone who has searched you has been temporarily disabled.
- Turn on timeline review to review posts that friends tag you in before they appear on your timeline
- To stop Facebook from tracking your location, change to 'Never' under 'Location' in your app settings or your phone's location permissions
- Instagram:
  - If your account is public, anyone will be able to like or comment on your posts and see or follow your profile
  - It is a good idea to make your Instagram account private so only people you confirm can follow you and see your profile
  - Tap  above your post to turn commenting off on an individual post (this will hide any existing comments)
  - Instagram uses 'geotag' to track where every photo was taken – you can disable access to your location by removing the location permissions on your phone
- Twitter:
  - Twitter's default setting is public which means anyone in the world can search, view and interact with you tweets
  - In your privacy setting you can select 'Protect my tweets' so only your followers can view your tweets (and you will get requests that you can accept or deny if someone wants to follow you)
  - Choose a name on Twitter that isn't your actual name
  - 'Geotag' is also a feature on Twitter, identifying where you send tweets from – unless you have turned it on, it will be off by default
- Snapchat:
  - Your Snapchat profile is only viewable to those you add as friends
  - Snap stories can be visible to 'everyone', 'friends only' or a custom group
  - You can choose whether 'everyone' or your 'friends only' are able to send you Snaps
  - When you sign up with your name and a username, be aware that these will both be visible to all other users – it is a good idea not to use your full name
  - On your birthday, a birthday cake emoji will appear by your name, but it is possible to disable this under your settings
  - Even if you send a snap for three seconds, a screenshot can still be taken (and there are apps that stop you getting a notification) and re-posted to other websites
  - SnapMap lets other people see your location while you are using the app – for your safety it is important to only share your location with your closest friends or choose Ghost Mode so no one can see your location

## *Where can you go for help?*

- Contact Netsafe for advice and support:
  - Using their online form at [www.netsafe.org.nz/report](https://www.netsafe.org.nz/report) (or click on 'Report Online Incidents' on their homepage)
  - Email: [help@netsafe.org.nz](mailto:help@netsafe.org.nz)
  - Free phone: 0508 NETSAFE (638 723)
  - Txt 'Netsafe' to 4282
  - If you are concerned about your or someone else's immediate safety call 111
- ICON is a web tool developed by Sticks n' Stones that supports you to understand and take charge of your privacy settings:
  - Website: [www.icon.org.nz/taking-charge/](https://www.icon.org.nz/taking-charge/)
- If an organisation has interfered with your privacy you can complain to the Privacy Commission:
  - Complain online: [www.privacy.org.nz/about-us/contact/enquiry-form](https://www.privacy.org.nz/about-us/contact/enquiry-form)

# THANK YOU!



## WRAPPING UP

- Hand out the evaluation forms: make sure everyone fills one in.
- Thank everyone for participating. Find your own way to wrap up the class.
- Remember to link people in with their local Community Law Centre or YouthLaw if needed.
- Follow up on any questions or issues: bring the correct answers to your next class.
- Make sure to pass on any feedback you have about this module to: [info@wclc.org.nz](mailto:info@wclc.org.nz)
- Have a rest!

# Risky business

## SCENARIO #1

You get sent a dick pic from a boy in your class. He messages you again asking for a nude.

## SCENARIO #3

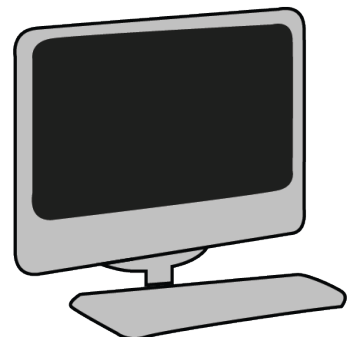
You videoed a fight that your mate Jono was involved in with students from another school.

## SCENARIO #2

Your friend sets up a group chat with all the girls in your class to talk about Miranda, who she says is a slut because she flirted with her boyfriend. She tells you on the group chat to back her up and send Miranda a message calling her out.

## SCENARIO #4

You have your Facebook profile set to public. Your account is set up under your full name and your birthday, phone number and email address are on your profile.





## ACTIVITY #1

# Risky business

Ask your group:

- Could someone use this to hurt me or could it hurt someone else?
- Would I be upset if this was shared with others?
- What's the worst that could happen if I shared this?

Ask your group:

- Could someone use this to hurt me or could it hurt someone else?
- Would I be upset if this was shared with others?
- What's the worst that could happen if I shared this?

Ask your group:

- Could someone use this to hurt me or could it hurt someone else?
- Would I be upset if this was shared with others?
- What's the worst that could happen if I shared this?

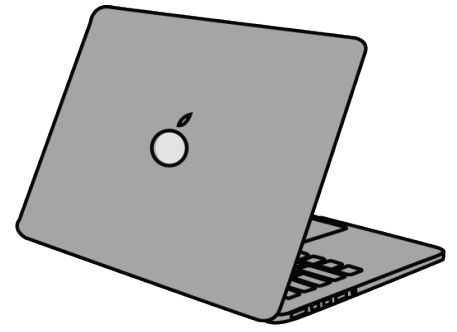
Ask your group:

- Could someone use this to hurt me or could it hurt someone else?
- Would I be upset if this was shared with others?
- What's the worst that could happen if I shared this?

## ACTIVITY #2

# What now?

Read the scenarios below and come up with all the different things you could do to keep yourself safe.



## SCENARIO #1

One of your friends uploads a photo to Instagram of you in your undies. They had taken it when they walked in on you getting changed at a sleepover. You thought it was a joke and they weren't going to do anything with it, but you feel really embarrassed.

What can you do?

- 
- 
- 
- 
- 
- 
- 

## SCENARIO #2

Someone sends you an anonymous message through an app "I guess the secret is out!" with a link to a page. The link takes you to a page someone has made about you. There are lots of comments from different people discussing rumours about all the boys you've been getting with. It has been going on for weeks. You feel humiliated and depressed as a result of the discovery.

What can you do?

- 
- 
- 
- 
- 
- 
-

ACTIVITY #3

Pick a path

CONTACT YOUTH LAW  
OR VISIT YOUR LOCAL  
COMMUNITY LAW CENTRE

ACTIVITY #3

Pick a path

CALL THE POLICE

ACTIVITY #3

Pick a path

TALK TO A TRUSTED ADULT

ACTIVITY #3

Pick a path

CALL A SUPPORT SERVICE



ACTIVITY #3

Pick a path

COMPLAIN TO THE  
DISTRICT COURT

ACTIVITY #3

Pick a path

# TELL YOUR SCHOOL

ACTIVITY #3

Pick a path

CONTACT YOUTHLAW  
OR VISIT YOUR LOCAL  
COMMUNITY LAW CENTRE

## ACTIVITY #4

# Logosketch

---

Sketch the logos of as many social media apps as you can think of!

Pick one and come up with your Top Privacy Tip for that app.

TOP PRIVACY TIP

