

# Social Media and Online Safety



# Contents

---

<b>What is this booklet about?</b>	<b>3</b>
------------------------------------	----------

---

<b>Section One: Top online safety tips</b>	<b>5</b>
--	----------

---

<b>Section Two: Personal information</b>	<b>6</b>
--	----------

What is personal information?	6
-------------------------------	---

Keeping your personal information safe	6
--	---

---

<b>Section Three: Ways of using the Internet</b>	<b>8</b>
--	----------

Email	8
-------	---

Searching for information	8
---------------------------	---

Using the internet at work	9
----------------------------	---

Online banking	10
----------------	----

Online shopping	10
-----------------	----

Subscribing to online services	11
--------------------------------	----

Online dating	12
---------------	----

<b>Social media:</b>	<b>13</b>
----------------------	-----------

• Facebook and Messenger	13
--------------------------	----

• Twitter	15
-----------	----

• WhatsApp	16
------------	----

• Snapchat	17
------------	----

• Instagram	18
-------------	----

• YouTube	19
-----------	----

• Video-calling – Facetime, Skype and Zoom	20
--	----

• Pinterest	20
-------------	----

---

<b>Section Four: How to stay safe online</b>	<b>21</b>
--	-----------

What kinds of things could go wrong online?	21
---	----

Cyberbullying	21
---------------	----

Cybercrime	23
------------	----

Personal Safety – Online Grooming and Personal Sexual Content	25
---	----

---

<b>Where to get help and information</b>	<b>26</b>
--	-----------

## What is this booklet about?

---

This booklet is a practical guide to help you use the internet and social media in a safe way.

The internet, email and social media can be useful and fun.

You can:

- meet new people
- chat with friends
- play games
- stay up to date with news and information
- learn new skills and be creative by watching videos and doing courses
- use email for talking with family, friends and services.

You might also need to use the internet, email, and social media for your job.

But sometimes people can experience problems when they use the internet and social media.

For example:

- you can be bullied or get upset by things people say
- other people can be hurt or upset by things you say or do
- people could take advantage of you by:
  - stealing money from you
  - telling you to send them photos of yourself
  - saying you should meet them and then hurting you.

It is very important to know how to keep yourself safe when you are on the internet.

This includes whether you're on a computer, a tablet such as an iPad, or on your phone.

This booklet has information on how to use the internet and social media, and how to stay safe. The booklet is long, and you may want to read it over a few days. The booklet may not have all the information you need. But it can be a starting point for getting more information. If you have worries about a situation you are in you should always make sure you get help from someone you trust.



This booklet has four sections.

**Section One: Top Online Safety Tips** is a one page list of the most important safety tips in the booklet.

**Section Two** explains what personal information is and how to keep it safe.

**Section Three** explains some of the ways that people use the internet, including social media, email, online banking, shopping and dating. It tells you what to look out for with each one.

**Section Four** is about how to stay safe online and why it is very important to look after your personal information to help you stay safe.

There is information throughout the booklet on what to do and who to talk to if you need help. There is also a help and information contact list at the end of the booklet.

## Section One: Top Online Safety Tips

---

### 1. Keep things private

- Be careful about sharing your personal information, including where you live, and where you go to school or work.
- Use passwords that people won't be able to guess.
- Don't tell other people what your password is.

### 2. Be respectful

- Remember that other people can see almost everything you do or say on the internet
- Be kind and friendly online
- Be careful what you say and share
- If someone is not being kind to you then you can block them. You can take a picture of their message and report them.

### 3. Make sure your internet is safe

- If you use a computer that doesn't belong to you, always log out when you have finished.
- Don't use public computers or public WiFi to do online banking or shopping.
- Don't click on links in spam emails (see page 11) or in website pop-ups.
- Only use websites and apps where you feel safe.

### 4. Know who you can trust

- If a stranger or someone you don't like sends you a friend request, you should say 'No'.
- Always talk to someone you trust when:
  - you don't understand something and need help,
  - you are being bullied or threatened,
  - you think something is a scam,
  - you think someone online is pretending to be a friend so they can take advantage of you.
- Never go on your own to meet a person you have met online, even if they seem nice or you think you know them. Tell someone you trust that the person wants to meet you. Call the police if you feel like you are in danger.

Remember to enjoy the internet. Have fun but use these tips to help you stay safe.

## Section Two: Personal information

### What is personal information?

Personal information is information about you such as:

- your image (photos of you)
- your name and date of birth
- where you live
- where you work or go to school
- your bank account details
- your medical information
- who your family members are.

People who don't know you can use this information to commit crimes, steal money and take advantage of you. You must keep this information as safe as possible. This means not sharing it with people you do not know or trust.

### Keeping your personal information safe

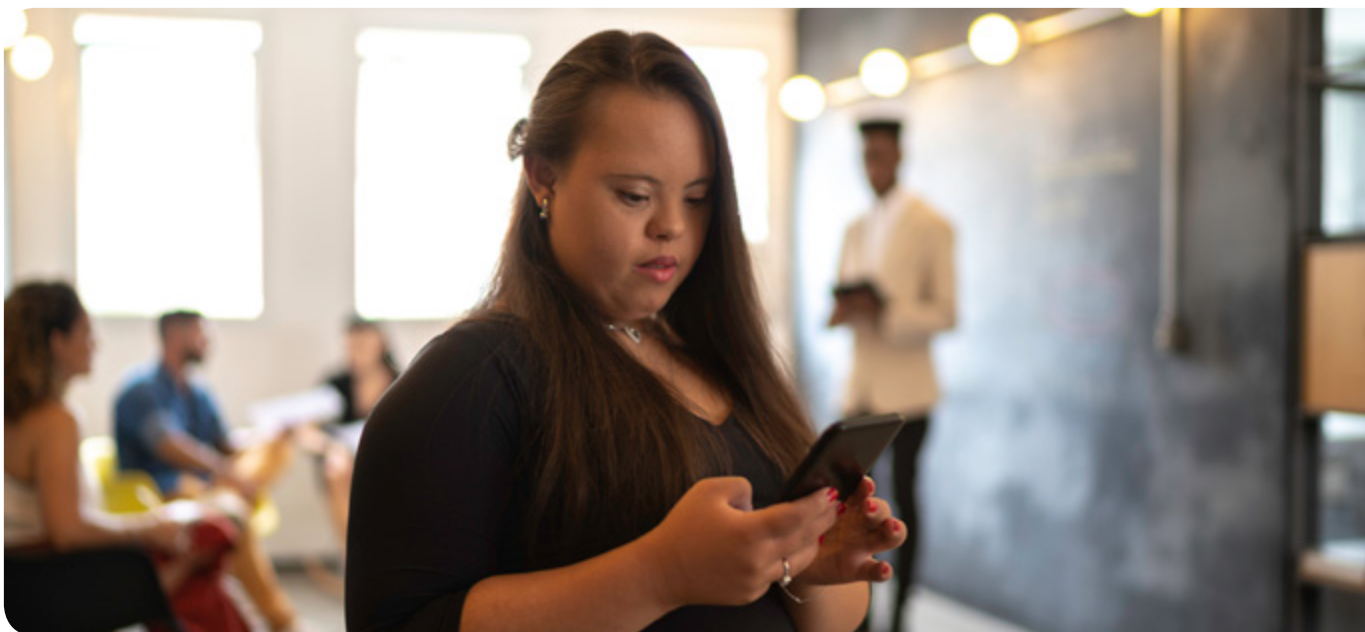
When you use the internet or join any of the different types of social media, you often need to set up an account. You will need to give them personal information when you set up your account. This is called a 'profile'.

A profile page is all about you. Other members of the website or social media app will be able to see some of the information you put in your profile. So you need to think carefully about what information you put in your profile



#### Useful privacy tips for setting up a profile:

- Start with only giving as little information as you can on your profile page. You can always add more later if you want to.
- Don't put personal information such as your address or phone number
- Don't add photos of yourself unless you know who can see them
- If you aren't sure what to put in, ask someone you trust to help you.
- Find out how to make your profile private so only your friends and people you trust can see it.



## Passwords

When you set up an account and profile you will need a password too. This is a word that you will use to get into the website or social media app.

Only you should know your password, so other people can't use it to get into your accounts. You need a safe password that other people can't guess.

You can use a mix of letters and numbers. Some websites or social media will have rules about using some upper case (capital) letters and having some numbers and characters, like \$ or &, in your password.



### Password tips:

- Don't use your date of birth, the name of your pet, or where you live. People could easily guess these.
- Use a mix of letters and numbers to make your password harder to guess.
- Don't use the same password for all your website and social media accounts.
- Try using an app that stores all your passwords safely and you only have to remember one to get into all your accounts. Examples of these apps are LastPass and Dashlane.
- Keep your passwords safe and don't tell other people. You might want to share passwords with a parent, but don't share them with friends.

## Anti-virus/malware protection

You can help make your computer and phone safer by making sure you update your software often and install anti-virus and anti-malware software. Ask someone you trust to help you if you need it.

## Section Three: Ways of using the internet

---

This section has information about the main ways people use the internet.

It includes:

- where and when to use the internet
- what the different websites are used for
- tips on what is useful and what to look out for to stay safe.

### Email

Email is a quick and useful way to communicate. You can use an email account with the company that provides your internet service. Or you can set up free email accounts online such as Gmail and Yahoo.

As well as typing a message to send, you can attach information files and photos. Lots of people sign up to get newsletters and to get special offers sent to them. But you can end up with lots of emails in your inbox everyday and it can be hard to work out what is useful and what is safe to open.

Unfortunately, there are criminals who use emails to try to get your personal information. This is called spam. Email accounts usually have a 'spam filter' that automatically send spam emails into a separate inbox. But sometimes spam can still end up in your inbox, so you need to be careful about what you open. Some spam can look very genuine but you should never give out personal information or your passwords in reply to an email. There is more information about Cybercrime in Section Four.

If you get an email or message that looks like spam, don't click on the link in the email. This could let cybercriminals get access to your information. Clicking on a link could also let in a 'virus' that could damage your computer.

If you aren't sure if an email is spam or not, show someone you trust such as a parent or if you are at work, your employer or a workmate.

### Searching for information

The internet is a really powerful way to find information about anything! You can type some words into your search engine (for example Google or Yahoo) to find what you are looking for. People often call this 'Googling', even if they aren't using Google. You will get lots of different websites to look through, and it might give you exactly what you need. Sometimes you might need to try putting in some different words to find the right information.

If you know the exact website address, you can type this in and this will take you straight to the website you want to look at. If you have some websites you like to look at regularly, such as your footy team website, your search engine will remember this and help you put in the address or you can save them in your browser. These are called *favourites* or *bookmarks*.

### Things to look out for:

It is important to know that anyone can put information on the internet, so what you read may not be accurate or true. If you aren't sure, ask someone you trust to help you work out what information is ok. Government websites and official organisations usually have more accurate information than blogs or forums.

Watch out for fake websites that pretend to be a reliable organisation. They could be trying to scam people. If a website doesn't look right, don't open it. You can ask someone for help if you aren't sure.

Be careful what you **download**. Sometimes website ads will flash or pop up and ask you to vote for your favourite singer or TV show, or offer you free downloads of emojis, or ask you to enter a competition. They will ask for your email address and then you will get lots of spam that could try to get your information or damage your computer.

**Don't give your email or personal information and don't download free offers.**

### Using the internet at work

Some people use the internet as part of their job. You may be comfortable using the internet at home and on your phone, but most workplaces have their own rules about what you can do online while you are at work.



#### Tips on using the internet at work:

- Most workplaces don't like you to use work computers for personal use, such as social media or looking up information that isn't part of your job.
- Some workplaces say you can only use the internet during your break times. Some workplaces might also have rules about making phone calls or sending text messages during work time. The internet can be a big distraction and use up time when you should be working.
- Some workplaces are ok with people using work computers for personal use during breaks, but others say you should use your own device such as your phone or iPad.
- Some workplaces don't mind you using the work computer for personal emails, but others say you shouldn't.
- Ask what the rules are where you work, so you know what is and isn't allowed. Ask someone to explain them if you aren't sure what all the rules mean.


## Online banking

Most people do their banking online these days. It is very convenient to look up your bank account to see how much money you have. It is very useful for paying bills online too.

But criminals try to **hack** into people's online bank accounts, so if you are using online banking, do it as safely as possible. There is more information on Cybercrime in Section Four.



### A few tips for online banking:

- Make sure it is the real bank website. Type in the address and look for the  **locked padlock sign**.
- Set a strong password and don't tell anyone what it is. Don't save your password on your computer.
- Don't let your computer save your username or password.
- Always log out of online banking when you have finished.
- It is best not to use public computers or log in to public WiFi to do online banking or make online shopping payments. **Hackers** can get your personal details easily.
- If you do online banking in public, make sure no-one can see your screen and steal your details.

Stay Smart Online has more useful information about safe online banking:

 <https://www.staysmartonline.gov.au/Protect-yourself/Doing-things-safely/Online-banking-payments>

## Online shopping

Online shopping is very popular. You can buy almost anything online, from books and music to toilet paper! You can order your groceries online and have them delivered, and send flowers or gifts to your family and friends. Some online shopping websites give you different ways of paying, such as credit or debit cards, and sometimes you can pay in instalments over a certain period of time.

But there are some things to watch out for when you are thinking of shopping on the internet:

### Fake websites

These can look like genuine online shops, with stolen logos, photos and company information. They are often selling luxury items, such as designer shoes and bags. But some are selling fake items, and some just want your money and won't send you what you have bought. Watch out for websites that seem to be selling items at a price that is very cheap.

Also watch out for websites that ask you to pay into a bank account or ask for you to send a pre-loaded money card. Real websites won't ask you to pay in these ways.

Real websites have a secure payment page where you can choose how you pay such as by **PayPal** or credit card.

Fake shopping websites often appear on social media such as Facebook ads. **Look at people's comments to see if the website is genuine or a scam.** Only buy from online stores that you **know** you can trust.

### Returns and refunds

A big problem with online shopping is you can't be sure the item is right for you until you get it. For example, you can't try on clothing or shoes like you could in a real shop. If the item doesn't fit, doesn't do what you thought it would or it doesn't look like what you saw on the website, you should be able to return it.

But, it is important to read the shopping website's policies (rules) before you order anything. Some say you can only return items if they are faulty, while others say you can only exchange an item, not get a refund. Most shopping websites have a time limit for you to send things back – often this is 30 days, but it could be less. And you will have to pay postage to return an item.

### Subscribing to online services

Online services can include all kinds of things. You can subscribe (sign up) to download music, movies, sport and TV shows. Or you might sign up for diet and fitness programs or to read your horoscope every day. It can be fun and exciting to get all these things straight to your phone, iPad or computer.

But most services are not free. Even if they start off with a free 'trial period', you usually have to pay for an ongoing service. This might be a yearly payment or monthly, and you might not realise how much it will add up to. Once you have signed up and given your personal and payment details, it can be difficult to stop the payments coming out of your bank. **It may even have been a scam and you are paying for nothing.**



#### A few tips about online services:

- Think about whether you can afford the service, or if you really need it.
- Is it value for money?
- Can you stop your subscription any time you choose to?
- If you think you'd like to sign up for an online service, it's a good idea to talk it through with a parent or someone you know will give you good advice.

Scamwatch has more information about shopping and subscribing to services online:

 <https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams>

Stay Safe Online also has some good information:

 <https://www.staysmartonline.gov.au/shoppingonline>

## Online dating

There are many websites and apps that people can use if they are looking for romance, whether it's for someone to go out with occasionally or a long-term partner.

Online dating may seem a good idea to help with meeting people, but there are risks including personal safety and scams. Even some of the websites that have been around a long time may not look after your personal information as safely as you would like.

Online dating websites can be expensive to sign up to. These dating websites are businesses that charge fees to help match people up.

Apps to help people meet up for dates are usually free, but you need to be aware of all the risks of meeting up with strangers and know how to stay safe.

Cybercriminals use online dating websites to target people for crimes. Sometimes they pretend to be your boyfriend or girlfriend, but they will tell you lies and ask you to send money or your bank details. More information on Cybercrime in Section Four.

Some people also use dating websites to target people for sexual purposes. They will ask to meet up with you for a date, but they just want to have sex and/or hurt you. More information on Personal Safety in Section Four.



### A few tips about online dating:

- Always talk to someone you can trust if you are thinking about online dating.
- Never give anyone on an online dating website your personal information, such as your address or bank details, and never send people money.
- People can make up a fake profile. You can't know if people are who they say they are.
- Never meet a stranger for a date by yourself, and never meet in places such as a private home. Choose a busy public place such as a café.
- Think about all the risks and whether on balance it is a good idea to use online dating. Ask someone you trust about other ways of meeting people safely.

Scamwatch has more information about online dating here:

 <https://www.scamwatch.gov.au/types-of-scams/dating-romance>

Stay Safe Online also has very good advice about online dating and using social media safely:

 <https://www.staysmartonline.gov.au/protect-yourself/doing-things-safely/socialising-online>

## Social media

Social media are websites or apps where you can connect to other people. Sometimes these are people you know and sometimes they are not. Different social media apps have different benefits, but it is important to stay safe while using all of them.

These risks are the same for all social media apps:

- People can see your personal information, so be careful how much you share.
- Strangers sending you friend requests or messages and comments
- People copying your profile and pretending to be you
- Ads or scams from people trying to steal your money or information
- Seeing inappropriate or upsetting content
- Being bullied or upset by other people on the app.

## Facebook and Messenger

Facebook is a social network where you can create your own page about yourself. People can send you 'friend requests' and you can ask to join other groups. When you join each other's networks, Facebook lists these people as your 'friends'. Facebook friends can be different to real life friends.

You can post information, photos and videos on your page and your Facebook friends can see this. You can also post things onto your Facebook friends' pages and they can post on yours. Your Facebook page is sometimes called your 'wall'.

You can also join up to pages belonging to organisations. This could be things like news media for the latest news or pages on other things you are interested in such as your favourite celebrity's page, pages for TV programs you like, fan pages for sports teams and so on.





When you open up Facebook you will see these posts. This is called your 'feed'.

You can also use Facebook Messenger to send instant messages to one person or a group. This includes photos, videos and information in documents.

*The good things about Facebook are:*

- You can use it to keep in touch with family and friends, no matter where they are.
- It helps you to keep up to date with what's going on.
- It can be entertaining as people share funny videos and pictures.



**Here are some tips to help you stay safe on Facebook and Messenger:**

- Don't put too much personal information in your profile. Keep it to the minimum.
- Don't tell anyone your Facebook password.
- You can change your privacy settings in Facebook so that only your Facebook friends can see what you post. You can also say what other information people can see on your page.
- You can 'un-friend' anyone who is upsetting you.
- You can also block people so they can't see anything about you on Facebook, and you can't see them.
- You can report people or organisations' pages to Facebook if they are offensive such as saying bad things about people.

## Twitter

Twitter is a social media app where you can post public messages. These are called Tweets. You can choose to follow people on Twitter, and people can choose to follow you. This means you are able to see each other's tweets in your feed. Companies, organisations and celebrities are also on Twitter and you can follow them to read what they are saying.

Tweets can only be 280 characters long. This is all the letters, numbers and spaces that make up what you say. You can tweet photos, videos and links to other information. You can re-tweet something that has come up in your Twitter feed. You can also send private messages by Twitter.

*Some good things about Twitter are:*

- You can use it to express yourself.
- You can follow your interests and find out what is going on in the world.
- People post tweets that make you laugh.

*But there are things that people don't like about Twitter too, such as:*

- It can be harder to understand, because people change how they spell words, or leave words out, so their message will fit in 280 characters.
- You don't have as much choice as Facebook when it comes to who can see your posts.
- It can be hard to know what is true.



### Here are some tips to help you stay safe on Twitter:

- Make your tweets 'private'. This means only your followers can see them. The only other choice is 'public' – where anyone can see them.
- You can also choose to 'Protect my Tweets' in your settings. This will help to stop people who aren't your followers from finding your posts by searching Twitter.
- You can change your Twitter settings to stop inappropriate posts. You do this by blocking certain words in your settings. You choose the words.
- When you take a photo with your phone then post it to Twitter, anyone can use it to see where you are. So, make sure to hide your location in your Twitter settings. You can also remove location from all your tweets.
- Be careful who you connect with. It's a good idea to only communicate with people you know.
- People often put website links into their tweets. Be careful what you click on as they could be links to people trying to get your personal information or damage your computer. Make sure your computer has anti-virus software to protect you.
- Watch out for someone pretending to be you on Twitter! If it happens, you can report it to Twitter and ask them to remove the fake person.



## WhatsApp

WhatsApp is for instant messaging. You can send messages, pictures and videos with just one person or in a group.

*Some good things about WhatsApp are:*

- It's an easy way to send messages.
- Groups let you chat with lots of people at once.
- It's free to use over WiFi or using mobile data.
- You can make free voice or video calls.
- You have choices about how you can hide your personal information and your location.
- It's easy to block people.
- If you get a call from a number that isn't in your contacts, WhatsApp will ask if you know this contact or if you would like to report it as spam.
- You can report problems you have had with individual contacts or groups. Make sure to keep a screenshot or photo of the offending text/picture/video and provide as much information as possible to WhatsApp as they won't be able to see the message otherwise.



### Here are some tips to help you stay safe when you use WhatsApp:

- Don't share too much personal information in your chats.
- Use the WhatsApp privacy settings to choose who can see your messages.
- Be careful who you connect with. It's a good idea to only communicate with people you know.

You can find Frequently Asked Questions (FAQs) about WhatsApp here:

 <https://faq.whatsapp.com/en/general/>

## Snapchat

Snapchat is an app that lets you send a photo, short video or message to your contacts. But the 'snap' is only on your screen for a short time before it disappears, or until you tap the screen. Snapchat Story lets you share a sequence of snaps for up to 24 hours.

*Some good things about Snapchat are:*

- It's easy to send videos and pictures to friends.
- You can choose who sees your snaps.

*But people say there are some things they don't like about Snapchat, such as:*

- It shares your location unless you switch to 'ghost mode'.
- People can share your photos by making a screen shot of them.
- Being asked for sexual photos from people you don't know.
- It can be used for bullying.



### Here are some tips to help you stay safe when you use Snapchat:

- Only add people you know to your contacts list. Snapchat might suggest other people but be very careful who you add.
- Block strangers who try to contact you. It's also ok to block people already in your contacts list if they send you inappropriate snaps.
- Make sure you hide your location by turning on Ghost Mode. There is also a 'pen' option you can choose to block out things like street addresses and car registration plates that could help people work out your location and personal information.
- Be careful what you share, even with friends. Only share pictures that you would be happy to share with anyone.

You can find Snapchat's safety tips here:

 <https://support.snapchat.com/en-US/article/safety-tips-resources>

## Instagram

Instagram is an app for sharing pictures and videos. You can follow your friends, family, celebrities and companies on Instagram.

*Here are some things people like about Instagram:*

- You can be creative, making and sharing your photos and videos, as well as enjoy other people's creative images.
- You can follow pages of things you are interested in, including posts from online stores.
- It's a fun way to see what people are up to.
- You can choose whether to allow other people to share your posts.

*But people say there are some things they don't like about Instagram, such as:*

- People you don't know can follow you and make comments about what you post. This can include mean comments and bullying.



### Here are some tips to help you stay safe on Instagram:

- Only allow people you know to see your posts. Set your account to private. People can then ask to follow you, but you have to approve them.
- If people make offensive comments on your posts, you can easily delete their comments.
- If people you are following post things that upset you, you can choose to remove them completely by 'blocking' them. It means they can't see or find you on Instagram. You can also hide a person's posts in your feed. This is called 'muting'.
- Report any problems such as inappropriate posts or bullying directly to the Instagram Help Center.
- Even though you can buy things directly from Instagram, don't store your credit card details with them. If you spot something you want to buy, it's safer to follow the links to the online shopping website.

Here is the Instagram Help Center link:

 <https://help.instagram.com>

## 📺 YouTube

On YouTube you can watch and comment on videos. You can also create your own videos and even have your own YouTube channel.

*Here are some things people like about YouTube:*

- Learning new things from videos. You can find videos about just about anything.
- Following your favourite YouTubers – people who make and post videos regularly.
- Watching music videos.

*But here is what people don't like:*

- You can see inappropriate videos.
- There are lots of ads.
- Some people write mean comments about videos.



### Here are some tips to help you stay safe on YouTube:

- You don't need a YouTube account to watch videos on YouTube. You only need an account to upload a video or comment on a video. So you can watch YouTube without giving your personal information.
- Talk to a parent or other person you trust if you are thinking about posting something to YouTube. Never post videos of yourself in underwear or not much clothing.
- If you see something you don't like on YouTube, you can turn it off. Or report it.  
Here is how to report offensive videos:

 <https://www.wikihow.com/Report-a-Video-on-YouTube#Steps>

## Video-calling

Facetime, Skype and Zoom are some of the apps that let you make video and voice calls using the internet.

You can choose just to use voice call or use video as well so you and the people talking can see each other.

Facetime is only available on Apple devices.

You can use Skype and other apps such as Zoom on any computer or device, and you can have a call or online meeting with lots of people taking part.

Video-calling is great for talking to family and friends, even if they are overseas. It is free over WiFi, so many people use it instead of making phone calls.



### Tips for video-calling:

- Only people who have your phone number can call you. If someone calls you and you don't want to speak to them, you can press 'decline'. You can also block people very easily.
- You can choose just to use voice calling if you don't want people to see you.

## Pinterest

Pinterest is like an online pin board. You can save pictures and information you find online and pin them onto your Pinterest boards. You can have boards for different subjects such as fashion, sport or whatever you are interested in. You can also re-pin things from other people's boards.

*Some good things about Pinterest are:*

- It gives you good ideas about things you are interested in.
- You can save all kinds of things you like and keep them all together to look at later.
- You can share things with other people.



### Tips for Pinterest:

- Keep your boards private so that other people can't see them. You can do this with each board.
- Don't pin or share anything that is inappropriate or hurtful.

## Section Four: How to stay safe online

### What kinds of things could go wrong online?

Here are the main problems people can experience on the internet. Information about each issue tells you what to look out for and do to keep safe, and what you can do if it happens to you.

### Cyberbullying

This is like bullying, but it happens online. Some people use the internet to upset and bully other people.

*Here are some examples of cyberbullying to look out for:*

- People saying mean things in text messages and emails.
- People sending you messages, pictures or videos that hurt you or embarrass you, that make you feel bad or ashamed.
- People gossiping or spreading nasty messages about you.
- People pretending to be someone else online to trick you
- People excluding you, shutting you out.

*What can I do if I'm being cyberbullied?*

Leave any groups or chats where people are being mean and upsetting you.

Keep copies of messages or photos that have been sent to make you feel bad. **You could take screen shots or photos or print them.**

Don't reply to the person who is bullying you. Don't say bad things back to them, as you could also get in trouble.

Block the bully's social media and phone numbers so they can't contact you.

If the bullying is on social media, report it to the social media service. This website shows you how to report problems to the different social media services.

 <https://www.esafety.gov.au/complaints-and-reporting/cyberbullying-complaints/social-media-services-safety-centres>.

Show them the messages or pictures so they can see that someone is bullying you. Ask them to remove the bullying posts.



### Where can I get help?

Tell someone you trust about the bullying, so they can help you. This might be family, friends or a support person. Show them the messages or photos you have kept so you can talk about what to do.



You can contact the e-Safety Office. This is an Australian Government service that helps all Australians have safer, positive online experiences. The office can help with:

- a complaints service for young Australians who experience serious cyberbullying
- identifying and removing illegal online content
- tackling image-based abuse.

 <https://www.esafety.gov.au/esafety-information/esafety-issues/cyberbullying>

Not all online bullying is against the law, but when it is ongoing and becomes very serious there are laws that can be used to punish the people doing it. You can find information on your local Police website or call 131 444.

You can also report serious cyberbullying to the Australian Cybercrime Online Reporting Network (ACORN).

 <https://report.acorn.gov.au>

Remember – Cyberbullying is **never** OK. People should always respect you. This also means we need to respect other people when we are online.

Here are some ways we can all be kinder and more respectful to each other:

- Check messages and social media posts before you send them, to make sure they won't hurt anyone.
- Don't share anything that could upset someone. This could be things like comments, gossip, cruel jokes, messages, photos or videos.
- Don't talk about anyone without their permission.

## Cybercrime

This is when people use computers to commit a crime.

*Here are some examples of cybercrime to look out for:*

**People hacking into your computer.** They do this to get into your online banking, email and social media accounts.

**Stealing your personal information.** They might do this to steal money from you or to pretend to be you, so they have a false identity for when they commit crimes. They might get your information by hacking into your computer or by getting you to share your personal information or passwords.

**Scams.** This is lying to trick people into giving out information such as bank details or paying for something that doesn't exist.

Look out for online scams where people are trying to trick you into getting your money or information. These can look like good news or a great opportunity. For example, you could get an email or message saying you've won a competition, when you didn't enter any competitions. Or they might say you've inherited some money and you need to send your information, such as bank details.

Other scams can look like they are from an organisation you know, such as your bank or a government department. These kinds of organisations will never ask for your details or passwords like this, so they will be scams. **NEVER** give your information.

Beware of online surveys and quizzes that might be on websites. They can be ways of getting your personal information.

If you get an email or message that looks like it might be a scam, don't click on the link in the email. Delete it.

Other scams can be people getting to know you online and then asking you for money. Or people threatening to hurt you or people close to you if you don't send them money or do something for them.

*Here are some things that could mean someone has stolen your personal information:*

- You notice that your bank account or credit card has been used to buy things you didn't buy.
- You get bills for things you didn't buy.
- People say you have sent them emails asking them to send money, but you didn't send the emails.

## How can I stay safe from cybercrime?

- Make sure you only share the least personal information possible in your social media and website account profiles.
- Set your social media accounts to 'Private' so that only people you trust can see your information and anything you post.
- Make sure your passwords are hard to guess, and keep them private. Only share with someone who you trust, such as a parent or someone close to you.
- Don't accept friend requests from people you haven't met or you don't like or trust.
- Don't give away too much information about yourself on social media.
- Don't share where you are when you post on social media. You can also turn off location settings on your phone so that people can't track where you are.
- Always 'log out' of websites that you have signed in to. And remember to 'log off' when you have used a public computer, such as at school or at the library, so the next user can't see your information.



### Where to get help:

Tell the police if you have been scammed.

You can report scams to Scamwatch. This is an Australian government organisation that works to stop scams.

 <https://www.scamwatch.gov.au/report-a-scam>

Scamwatch can't help you personally, but there is information on where to get help if you have been scammed.

 <https://www.scamwatch.gov.au/get-help/where-to-get-help>

## Personal Safety – Online Grooming and Personal Sexual Content

Some cybercriminals use the internet to get to know people, including children, so they can try to have a sexual relationship with them or get sexual photos or videos of them.

### Online grooming

This is when the person trying to set up the relationship is being friendly and trying to get the trust of the person being targeted. They do this in different ways. They might say they are the same age as you and like the same things you do. They will say nice things about you to make you feel good. They might offer to buy you things and ask you to do things for them.



#### Important safety tips:

- Never share personal information, such as where you live or go to school or work, or photos or videos with someone you only have contact with online.
- Don't go to meet someone in person if they ask you to and if you think they have been grooming you.
- If something feels wrong, tell a parent or someone else you trust immediately.
- Tell the police.

You can report online grooming here:

 <https://www.thinkuknow.org.au/report>

### Personal Sexual Content

This is when people take photos or videos of themselves naked and send them to other people. It is sometimes called sexting.

Some people might share photos or videos of other people's personal sexual content, or threaten to share them with other people. It is never ok to do this. It is a form of abuse and can get people into serious trouble with the police.

ThinkUKnow has some good resources that cover online grooming and personal sexual content, including an Easy Read Guide for staying safe online.

 <https://www.thinkuknow.org.au/resources>

## Where to get help and information

### Police

 Call 131 444

Press '1' if you need a police officer to attend an incident now.

Press '2' to report an incident or for general information.

 Call 000 if it is an emergency

If you are at risk of harm and need urgent help call 000 and ask for the police. Tell the operator exactly where you are – the address or name of the location – so they can find you quickly.

Make sure your phone company has your current address. Emergency services sometimes use this information to find you.

### Lifeline

 Call 131 114

Lifeline has a free 24-hour telephone counselling service. Anyone can call Lifeline at any time.

Lifeline can also provide you with information about other support services available in your area.

 <https://www.lifeline.org.au>

### Beyond Blue

 Call 1300 224 636

Beyond Blue provides information and support to help everyone in Australia achieve their best possible mental health, whatever their age and wherever they live. This includes a 24-hour helpline you can ring to talk about anything that is making you feel anxious or depressed, including being bullied.

 <https://www.beyondblue.org.au/get-support/get-immediate-support>

### Youth Beyond Blue

 Call 1300 224 636

Youth Beyond Blue is a website about anxiety, depression and suicide, for young people aged 18 to 25. You can call their helpline to talk about cyberbullying and other online abuse and problems that are making you feel bad.

 <https://www.youthbeyondblue.com/understand-what%27s-going-on/bullying-and-cyberbullying>



## Kids Helpline

 Call 1800 551 800

Kids Helpline is a 24-hour, seven day a week counselling service for Australian young people aged between 5 and 25 years. Kids Helpline talk to more than 6,000 kids each week about all sorts of problems. Young people can access Kids Helpline by calling 1800 551 800 or visiting their website:

 <https://kidshelpline.com.au>

## ThinkUknow

ThinkUKnow is a partnership between the Australian Federal Police, Commonwealth Bank, Microsoft and Datacom. They work with all state and territory police and Neighbourhood Watch Australasia to run presentations for parents, carers and teachers and young people from Kindergarten to Grade 12. The cyber safety presentations sensitively cover a range of topics including sexting, cyber bullying, online child exploitation, online privacy, and importantly what to do when something goes wrong.

 <https://www.thinkuknow.org.au>

They have some very good free resources including an Easy Read Guide to staying safe online:

 <https://www.thinkuknow.org.au/resources>

## National Centre Against Bullying

National Centre Against Bullying has advice and resources suitable for young adults, parents and teachers on a variety of topics.

 <https://www.ncab.org.au/bullying-advice/>

## Scamwatch

Scamwatch is a government website that has useful information about how to recognise, avoid and report all kinds of scams.

 <https://www.scamwatch.gov.au/about-scamwatch>

They have a list of links for where to get help:

 <https://www.scamwatch.gov.au/get-help/where-to-get-help>

## Stay Safe Online

The National Cyber Security Alliance runs this website that has some very good information resources:

 <https://staysafeonline.org>

## eSafety Commission

This is the federal government department that oversees public and private organisations working to keep Australians safe online. There are some good information resources on the website.

 <https://www.esafety.gov.au>

## GoDigi

This national program is designed to help people across Australia get online. The GoDigi website offers a variety of technology tools, guides, events listings, mentoring and a searchable database of places that offer face-to-face training. Find out more: go to

 <https://www.godigi.org.au>



Down Syndrome  
Australia



1300 881 935



18/71 Victoria Crescent, Abbotsford VIC 3067



[info@downsyndrome.org.au](mailto:info@downsyndrome.org.au)



[www.downsyndrome.org.au](http://www.downsyndrome.org.au)