THINK U KNOW .org.au

PARENT & CARER SOCIAL MEDIA STARTER KIT:

Preventing online child sexual exploitation

Australian Centre to Counter Child Exploitation

AFP AUSTRALIAN FEDERAL POLICE

ABOUT THIS GUIDE

Parents and carers,

This starter kit has been created for when your child is beginning to sign up for social media apps and sites.

It includes advice on what to consider when creating social media accounts, potential challenges relating to certain features on social media, as well as tips and advice for ongoing social media use to prevent online child sexual exploitation.

Meeting people, making new friends and interacting online is common through social networking platforms.

Unfortunately it can be easy for someone to lie about their online identity and it can be difficult to prove someone is who they say they are.

Challenges such as self-generated child sexual abuse material, inappropriate contact, online grooming, and coercion and extortion can take place on any interactive app or site.

Our focus is on the importance of providing education and tools for young people to use the internet safely, including recognising when something isn't right and taking action.

ThinkUKnow

- **ThinkUKnow Australia**
- **ThinkUKnow_Aus**
- **ThinkUKnowAUS**

Australian Centre to Counter Child Exploitation

- **ACCCEaus**
- **ACCCE_AUS**
- **ACCCE**
- **accceaus**

What is social media?

The internet and connected devices allow people to meet and connect online, this can be through social media. Social media includes websites and apps that allow users to create and share content and participate in social networking.

Social media allows your child to generate their own content, including status updates, comments, images, and videos. Your child can share these on their own accounts for other people to engage with. They might also comment or 'like' a post on another person's 'wall', page, account or forum.

Why 13+?

Age restrictions on social media apps come from US legislation 'Children's Online Privacy Protection Rule' or 'COPPA'.

COPPA imposes specific requirements on operators of websites or online services directed to children under 13 years of age; some examples include requiring verifiable parental consent and allowing parents to review personal information collected from their children.

Although at age 13 a young person is legally allowed to create a social media account in their own name, it does not necessarily mean that the content and images they will see is appropriate for that age group. For more information, view the **US Federal Trade Commission's rules**.

To report online child sexual exploitation

Report online child sexual exploitation via the **Report Abuse Button** on the Australian Centre to Counter Child Exploitation (**ACCCE**), Australian Federal Police (**AFP**) or **ThinkUKnow** websites:

Report abuse

All reports are assessed by the AFP-led ACCCE Child Protection Triage Unit.

If you believe a child is in immediate danger, contact Triple Zero (000).

For non-emergency situations that still require a timely response, contact your local police station or call 131 444.

If you prefer to report in-confidence, visit **crimestoppers.com.au** or call 1800 333 000

If you or someone you know is affected by physical child sexual abuse or exploitation including historical child sexual abuse, please report to police in your relevant state or territory.

Support

If you or someone you know are impacted by child sexual abuse or online child sexual exploitation, there are **support services available**.

Child sexual abuse material or other offensive and illegal content can be reported to the eSafety Commissioner who will work to remove it. Report online at **esafety.gov.au/report**.

SIGNING UP: WHAT TO CONSIDER

This section looks at a number of proactive measures parents and carers can put in place when signing up to social media to prevent online child sexual exploitation.

Some apps have more safety features than others or have varying sign up and verification processes in place.

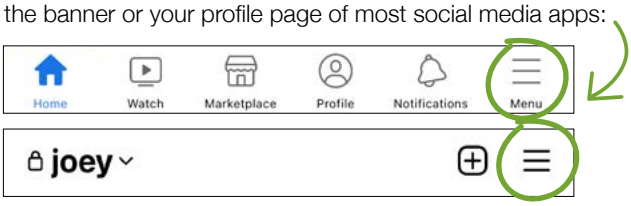
We always recommend doing your own research in determining whether an app or site is suitable for your child.

Limiting the information your child could be sharing online, either knowingly or unknowingly is one way to reduce inappropriate contact from others.

Privacy settings

We recommend the **strongest privacy settings for young people** so that their information is not publically viewable, which may limit the risk of contact from unknown users.

While privacy settings vary depending on the app your child is using, the settings features are generally accessed by the menu option (appears as three lines or a settings icon) in the banner or your profile page of most social media apps:



TIP

Include your child during the sign-up process

Explain the reasons for your decisions and why you have these rules about their social media use. Encouraging open and regular discussion about their online activities will make it easier for your child if they need to come to you for help.

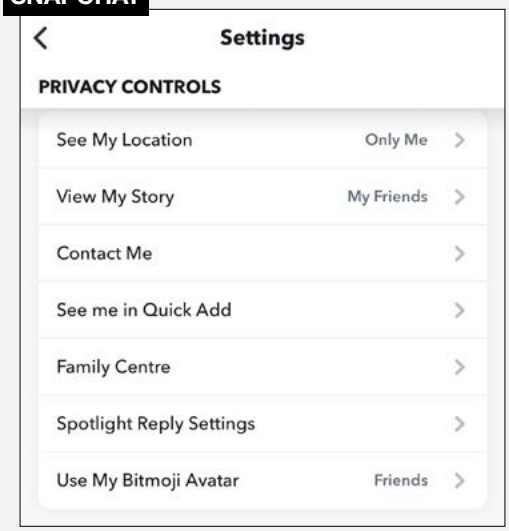
Key privacy settings that should be considered include:

Private account

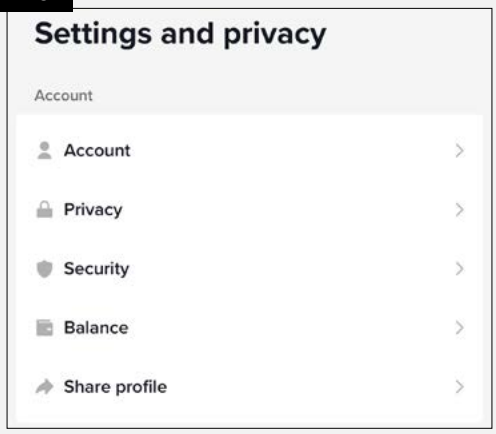
Private account means that new friends or followers will need to be reviewed and approved before they can access your child's account. Terminology differs across various platforms but look for options such as 'Private account', 'Who can contact me', 'How people can find and contact you'.

INSTAGRAM

SNAPCHAT



TikTok



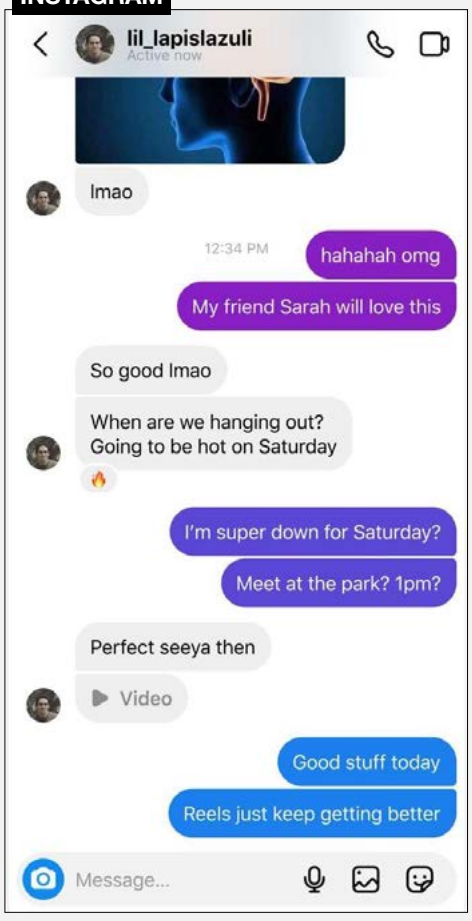
Friend or follower requests

Friend or follower requests can come from 'everyone' or 'friends of friends' (this means requests will come from people who are friends with those already on your child's contact list). Your child should only accept friend requests from people they know 'in-person'.

Direct message functions

Many social media apps come with a direct message function. If your child has public social media accounts this generally means anyone can send your child a message. Most apps have the ability to limit who can send a direct message request including only approved friends or followers. Some apps have the option to send message requests to a folder before being added to a chat list.

INSTAGRAM



Source: Instagram

Viewing friends or follower lists

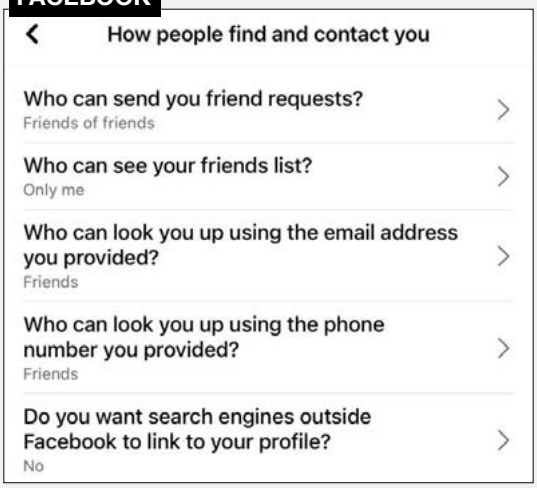
Check whether the social media app has the feature that allows only approved friends/follows to view your child's friend/follower list. Other options include 'public', 'friends' or customisable to not allow nominated friends. If your child were to befriend someone they met online, it would be relatively easy for this person to gather information about your child's friends and family if their social media account has open settings.

In cases of sexual extortion, offenders have been known to make threats to share content with friends listed on a victim's social media account. This can happen as a result of a child inadvertently giving access through 'public' social media accounts.

Tagging permissions and mentions

This provides the ability to choose who sees the post before a friend/follower tags your child in their photos and videos. Options can include 'everyone', 'people you follow' and some options allow you to review tags before they appear. Some apps allow for your child to select who can 'mention' their account in others' posts, stories, live videos and captions. Consider only allowing 'people you follow' (approved followers) or 'no one'.

FACEBOOK



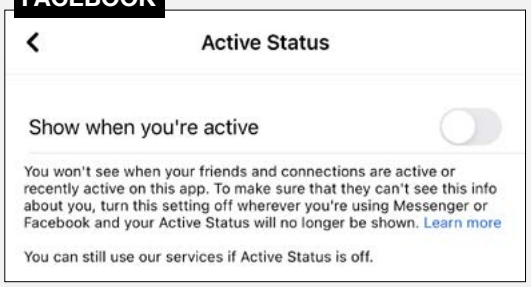
Publicly searchable account

Not all platforms give this option, but in some cases you can opt to remove the ability for your child's social media account or profile to be found on search engines. Note, this doesn't limit people searching for your child's name on the social media app itself.

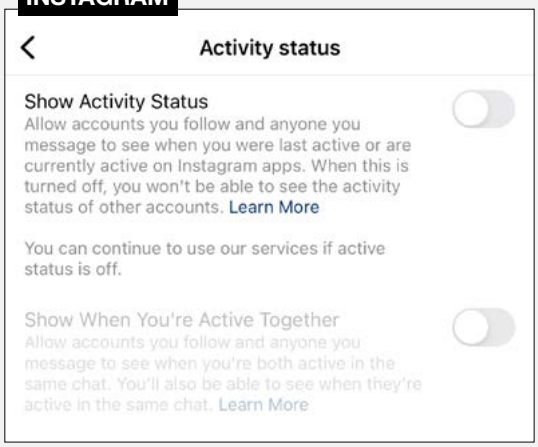
Activity status

This shows when your child is active on the platform, and when active shows other users with a small green circle next to your child's profile photo. This can be limited in some apps by selecting 'show activity status' and ensuring it is off.

FACEBOOK



INSTAGRAM



Privacy and safety are not a 'set and forget'.
We recommend checking in with your child to stay up to date on the apps they are using. Platforms often introduce new setting functions that can further add to increasing your child's privacy online. These will often appear as 'new' in the settings area.

Once you have agreed upon privacy settings, regularly check in with your children and make sure privacy settings are still active, as these can be changed back.

Note: Device settings are different from app settings. Geotagging occurs when a photo is taken on a smartphone/tablet, and it embeds the location/ date/time data into the image. This data can easily be accessed once someone has the photo. It is recommended to remove geotagging from your child's device settings (their tablet or phone) which can be accessed in your phone settings.

This can be done through **your phone settings**, **app settings,** and changing **camera and location** permissions.

Your child's bio/profile

The bio or profile can typically be found when you click on the profile username, and contains information about the account owner, including personal information.

Most social media platforms have a public profile and private profile. However, keep in mind that some apps by default make bio information public.

A public profile only shows information that the user has selected to be viewed publically. A private profile will be what the account owner has selected to be viewed by approved followers or friends.

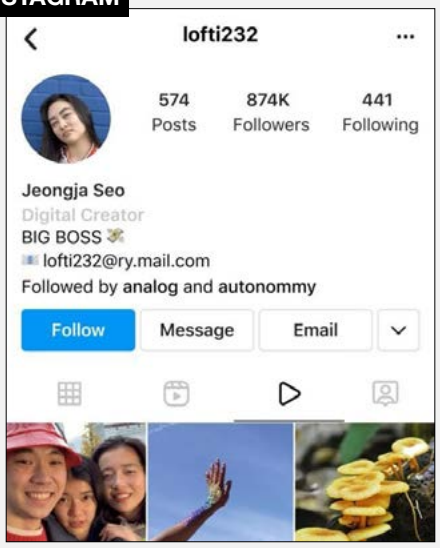
TIP

Ensure no personal identifying information is viewable from your child's public profile

Such as age or date of birth, location, school or their full name (consider using a slightly different name, such as your child's first and middle name rather than their first and last name).

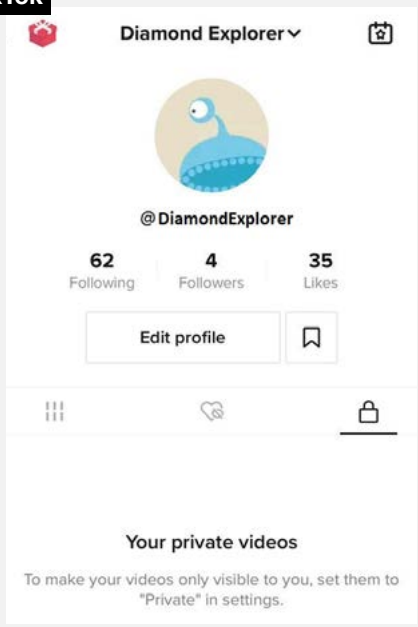
Keep in mind that accompanying profile photos can also contain personal information.

INSTAGRAM



Source: Instagram

TikTok



Choose smart usernames

Some social media platforms require a username which is often publicly visible.

When deciding on a username, encourage your child to use a smart username. Smart usernames are usernames that don't give away their name, age or where they live.

EXAMPLE

Username

Jack09Brisbane

Personal information:

Name is Jack, born in 2009 and lives in Brisbane.

VS

Smart Username

DiamondExplorer

No personal information

May relate to their favourite online game (in this case Minecraft)

Terms and conditions/ End-user licence agreements

Parents and carers should have a general understanding of what their child is signing up to and the agreements they have with social media platforms. While terms of service can be quite lengthy, we recommend you have a general understanding of the services your child is signing up to.

Most social media services have four parts to their terms and conditions:

- **A licence agreement** - This allows the service to change, add to, delete, publicly display, reproduce, copy, distribute, sell and use your personal information, including your photos, posts, private messages, comments and videos, without your permission.
- **Law enforcement disclaimer** – This means that companies can provide information that was posted online to police for investigation purposes.
- **Community guidelines** – This outlines the rules around how to use the service and consequences for breaking the rules, such as shutting an account down.
- **Privacy policy** – This explains what private information the company collects, how it is used, and what privacy settings you can use.

There are many online resources available that simplify terms and conditions for major platforms if you require more information on what these terms mean, and how they can affect your child's social media use.

STAYING SOCIAL MEDIA SMART

This section will explore tips and advice for managing social media accounts, including popular features found on social media platforms, to minimise inappropriate contact and recognise suspicious behaviour.

Posting/tagging

Posting and tagging is a core function of many social media platforms, and can be a way for your child to keep their friends updated on what they are doing and feeling.

Posting can either be in text, photo, and video form.

Tagging is when a user 'mentions' another user in their post or tags a location. Some social media platforms are built around this core function and offer tools to simplify this process (i.e. TikTok and its Duet and Stitch features which can be limited in account settings).

When sharing content or 'posting', it is important not to give away personal information.

Encourage your child to think critically by looking at the content before they post. Can they see identifying information, such as their street number, school name on their uniform, or the sports club they play at?

TIP

Post after leaving

Your child wants to post about a fun day out with a friend? Encourage them to post once they have left the location. Posting frequent locations or activities publicly can give away a lot of information about routine, hobbies or other interests.

Commenting or responding to comments

Commenting or responding to comments is another core feature of social media platforms.

There are many public pages or profiles where you can 'comment' and have people you don't know or people who aren't approved friends/followers reply to the comment.

Online child sex offenders may use public pages/posts that have a young audience to find potential victims. They may use a young person's comments on these pages/posts as an opportunity to interact.

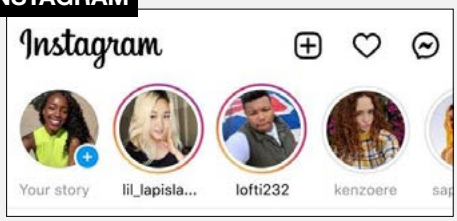
Stories

Stories allows users to upload a photo or video to their page, appearing at the top of their friends feed in the stories section and disappearing after 24 hours.

Apps such as Snapchat and Instagram offer a 'memories' feature of stories, where they will give a montage of what you shared for a particular month or event that you posted on your story.

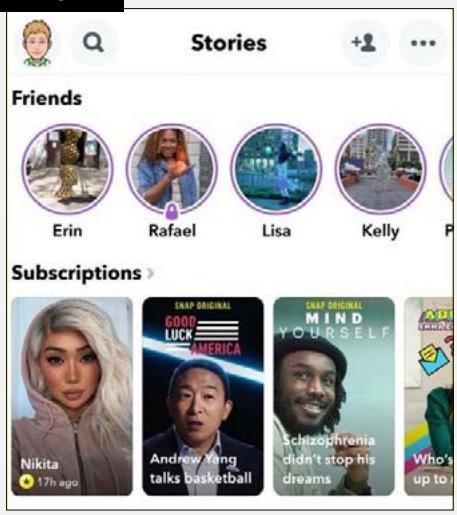
Stories can easily be saved by other users, by screen capturing or other software.

INSTAGRAM



Source: Instagram

SNAPCHAT



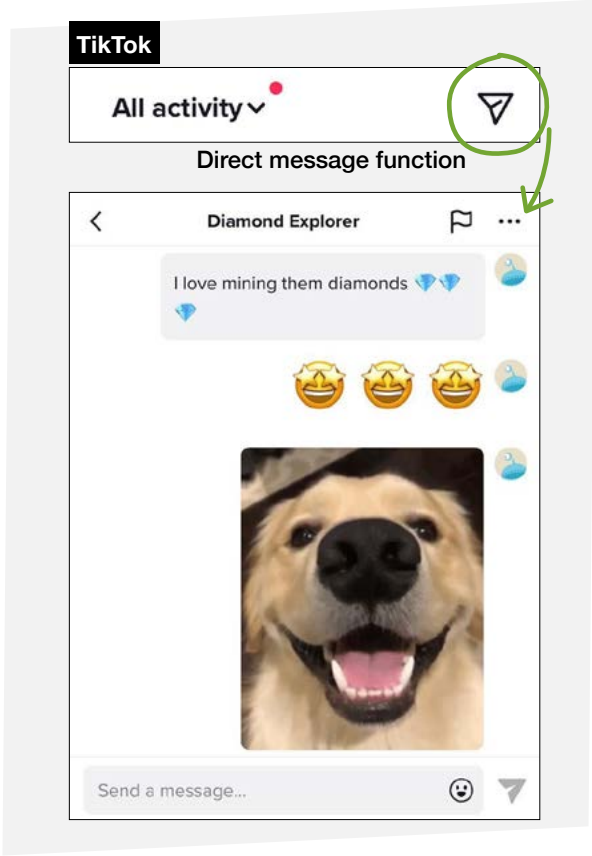
Source: Snapchat

Direct message

Direct messaging is a feature of social media platforms that allows users to message another user privately. For example, users can communicate in 'private' directly with each other, rather than on a public wall or forum.

The direct messaging feature often includes the capability to share videos, images, voice recordings, GIFS (moving images with no audio), user's location, and play games.

Depending on account privacy settings, if a user attempts to direct message another user they are not friends with, the message will appear as a 'message request', where the user can either accept, ignore, or block and report.



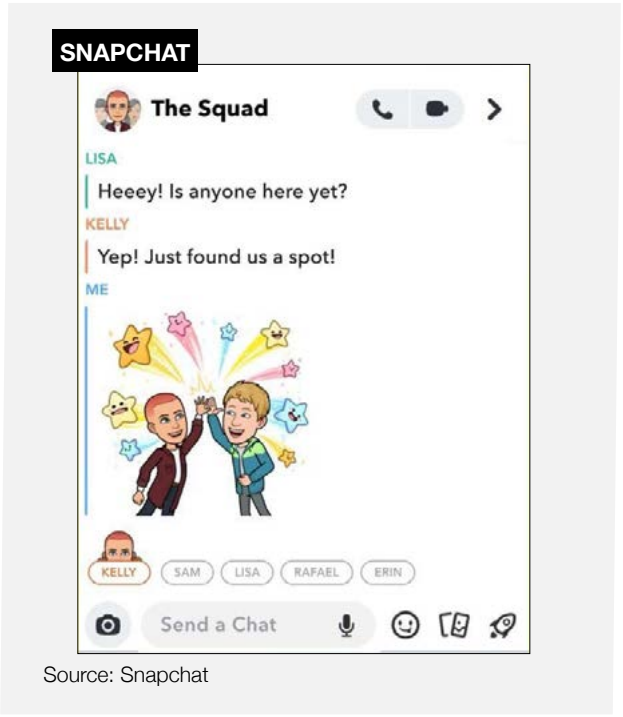
Group chats

Group chats are a feature that is an expansion of direct messaging.

Rather than messaging one user, group chats can include anyone invited to the chat. Group chats can occupy many different purposes, ranging from a school friends chat, a sports team chat, or gaming themed chat.

Group chats are a common feature for social media platforms, but they are not exclusive with other messaging services/applications that utilise this feature. Other messaging platforms include WhatsApp, Telegram, Discord (gaming themed) and Signal.

Group chats are a great way of communicating with like-minded people, but they pose their own set of challenges. Your child may not know everyone in the group chat and they may be talking to someone who is much older than them.



Source: Snapchat

RESEARCH

Market research commissioned by the ACCCE showed that:

95% of children aged 12-15 years old had access to a personal device

54% of these use messaging apps

For more information, view the **full report here**.

Going ‘live’

Live streaming and live video chat platforms continue to be popular with children and young people. Facebook, Instagram, Snapchat and TikTok all have these capabilities. Live streams can be public or private, depending on the privacy settings. Live streaming is popular for playing video games, Q&A sessions with friends/followers, or showing a specific activity.

Given that live streams are in ‘real time’, they can be unmoderated and unpredictable, and can increase the chance of exposure to content that is not age appropriate for your child. If your child wants to live stream, it is recommended to restrict viewing to friends/followers only.

INSTAGRAM

Police are seeing instances where online child sex offenders will trick a child into undressing and performing sexual acts on a live streaming platform, and will secretly record them and use the video to blackmail and threaten the child into providing more explicit material. This is called ‘capping’.

Disappearing media

Disappearing media has become a popular feature with social media platforms.

This can be in the form of ‘stories’ that can be viewed for 24 hours by your friends/followers or by direct messages that are ‘destructed’ after being viewed.

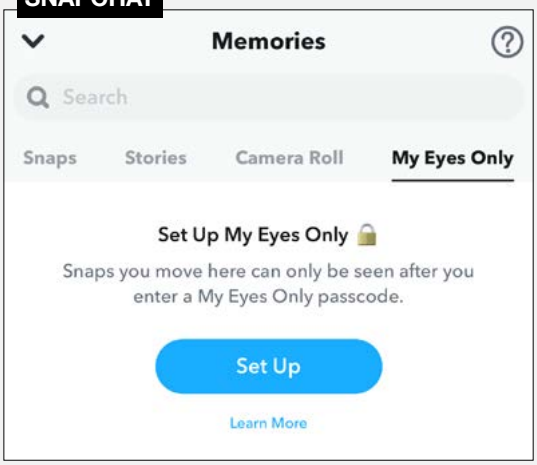
The popularity of this feature has increased because people are more likely to share content if they believe it will be deleted after a certain amount of time.

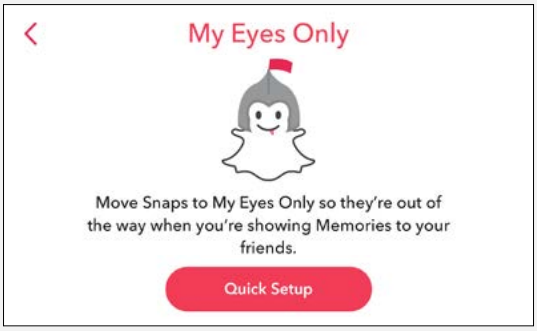
While the content may have disappeared, it can be relativity easy for other users to save the content without the original creator knowing. It is important to explain this feature to your child and the image or video they thought would be kept private can be captured without them knowing.

Secret storage photo galleries

Some social media platforms offer the ability to hide photos behind a password protected ‘vault’. One example is Snapchat’s ‘My Eyes Only.’ This feature allows the user to move saved photos into a password protected folder. The secret storage feature is one way a child may hide certain images or videos.

SNAPCHAT





Recognising suspicious accounts

Encourage your child to keep a lookout for friend/follower requests from 'suspicious' or random accounts. Suspicious accounts might have minimal contacts or followers, only have been active for a short time and use bad quality or generic 'stock' photos.

Online child sex offenders will often create fake accounts pretending to be a similarly aged child, and attempt to friend/follow other children.

Talk to your child about only accepting friend or follower requests from people your child knows in-person and encourage them to block suspicious requests.

Online friends and offline friends

In some cases, children who 'meet' someone online don't necessarily consider them strangers. To them, they may be just another real friend, particularly if the other person has deliberately sought out to develop an online 'relationship' or 'friendship'. This can particularly be the case in online grooming.

It is important that you remind your child that not everyone online is who they say they are. When they meet people online, they only know what the other person decides to share with them, which may not be true. Online child sex offenders can manipulate their story to align with your child's interests, and will use what your child posts as a way to initiate contact.

TIP

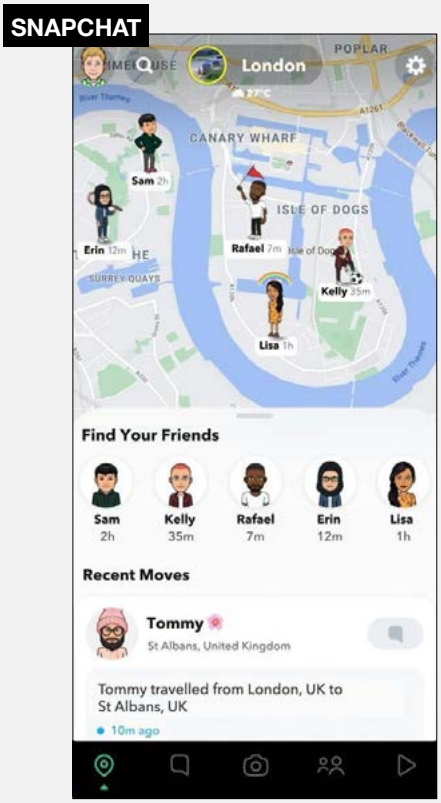
Review friends and followers

Sit down with your child and regularly review their friends or followers list. If you or your child don't know them in-person or 'offline', consider deleting them.

Location settings/ friends map

Some social media platforms include a 'friends map' feature. This feature shows a map where your friends are currently located and can include directions on finding your friend.

Most social media platforms have location settings which can show your friends or followers where you are. If your child is constantly 'checking in' at locations, people can use this information to build a profile of places they frequent on a regular basis.



Source: Snapchat

TIP

Turn off location services

Turn off location services for applications that don't require them to function. For example, map navigation apps will require location services to function correctly. You can find this in smartphone general settings under 'app permissions'.

SOCIAL MEDIA STARTER CHECKLIST

- ☐ Have a discussion with your child about how they will use social media
- ☐ Research the apps and sites that are most suitable for your child
- ☐ Include your child in the sign-up process
- ☐ Choose strong privacy settings
- ☐ Set up profiles and usernames that limit personal information
- ☐ Establish rules for approving new friends or followers
- ☐ Set boundaries and expectations through the **Family Online Safety Contract**
- ☐ Explain what to do when they need help, reassure them that nothing is too big or small
- ☐ Develop a system for regular privacy 'check-ups' to ensure privacy settings are still in place
- ☐ Stay up-to-date with new app features and functions for the apps your child uses

CONVERSATIONS TO HAVE WITH YOUR CHILD

- 🗨 Ask about their online activities, how they intend to use the app and who they will be interacting with.
- 🗨 Talk about what privacy settings are most appropriate. Keep in mind these can be changed by your child at any time so it is a good idea to regularly check in to make sure these are still in place.
- 🗨 Talk about critical thinking and how to recognise a suspicious friend or follower request – and what to do about it (block, and if necessary report).
- 🗨 Work out a plan for what they would do if someone online was acting suspicious, asking personal questions or even asking for sexualised images.
- 🗨 Make sure your child has a support network of trusted adults they can talk to if they feel unsafe or unsure.

GETTING HELP

This section will guide you on making a report and supporting your child.

Platform level support

If you are suspicious of an account, make a report to the platform and block the account.

If you believe the account was leading to an offence including online child sexual exploitation, make a report to police.

Australian Centre to Counter Child Exploitation

Online child sexual exploitation can be reported to the **Australian Centre to Counter Child Exploitation**.

There is no information too small or insignificant, and the information provided by you can hep to protect children online.

Call **Triple Zero (000)** or your **local police (131 444)** if you think a child is in immediate danger.

If you prefer to report anonymously, you can visit **Crime Stoppers** or call their toll free number: **1800 333 000**.

Making a report

When making a report, collect evidence before the content is removed to show police exactly what happened. This includes:

- Screenshots/photos of the conversation (remember to not screenshot, save, share or distribute any explicit images of the underage person as this is an offence)
- Record of social media details (including the suspect's account, profile, profile usernames and URL of profile)
- Webpage addresses (URLs)
- Dates and times
- Any other information you have about the interaction or suspect.

It is important to capture this information before blocking or deleting the user or you may lose important evidence.

► Support services

- **Kids Helpline** is a free, confidential telephone and online counselling service for young people between 5 and 25 years old.
- **Beyond Blue** is a service for connecting people with mental health professionals.
- **Headspace** is the national youth mental health foundation providing early intervention mental health services for 12-25 year olds.
- **Lifeline** is a 24-hour crisis support and suicide prevention service.
- **Reach Out** has information, stories, apps, online tools and forums to seek support.
- **QLife** is a national service that provides anonymous and free LGBTI peer support and referral for people wanting to talk about sexuality, identity, gender, bodies, feelings or relationships.

FURTHER INFO & RESOURCES

- ThinkUKnow has created a guide on parental controls and settings for popular gaming and smart devices.

  A copy is available on the **ThinkUKnow website**.

- For further specific information on apps and app settings, visit the **eSafety Commissioner website**.