ozchild
Every child deserves the chance to shine

Cyber Safety Manual

Basics and strategies for carers

2018 edition

www.ozchild.org.au

Introduction

The OzChild Cyber Safety Manual was created to help carers of children in out of home care to understand the significant risks posed by social media.

Device use (iPads, tablets, game consoles, computers and phones) and the internet are now a part of everyday life. The manual's main message is to not ban the internet or devices from children, but to be aware of the dangers and educate children. That way the whole family can remain cyber safe, through continued communication and education.

Children in care can tend to present with vulnerabilities due to their previous trauma history. It can affect the way that they trust others, in person and online, along with their level of understanding of the potential dangers in all social media applications. It is important for carers to have a level of understanding of social media and cyber safety basics, to be able to educate the children in their care.

This manual is aimed towards:

- Foster carers and Kinship carers.
- Carers who have a limited understanding of social media and the internet, or want to learn more about the internet and social media.
- Case workers who would like to learn more and use that knowledge when working with clients.

Contact us:

OzChild Foster Care Program
Level 4, 14-16 Mason st, Dandenong VIC Australia 3175.
PH (03) 9212 3900
www.ozchild.org.au

Author: Virginia Papadopoulos
E: vpapadopoulos@ozchild.org.au

Table of Contents

General Device and Internet Tips for Carers

The internet is a great resource for families and has become a major influence in the way people socialise**.** However it is important to be aware that there are ways to enjoy using the internet while still using strategies to protect children and young people in your care from identity theft, sexual predators, stalkers, and online bullying.

Here are some general cyber safety tips for families.

General Internet security

If required, Install proper security and parental controls on all the computers in your home. Parental controls can help filter what content children can access and see online, such as avoiding specific websites or sexual content. They can also help adults set time limitations regarding what times a child can use the internet. More information on Parental controls can be found at the Australian eSafety Commisioner's website here https://www.esafety.gov.au/education-resources/iparent/online-safeguards/parental-controls

Use internet passwords

Put a password on your internet connection, especially if it is a home wifi connection. See page 36 for instructions on how to change your home wifi password.
All homes should have internet that requires a password, whether your internet is Wifi or not. This prevents any unwanted users, like your neighbours, using your internet.
Carers who need to limit the internet time or more closely supervise internet time for the children in their care should change the password regularly. Alternatively, carers can disconnect the child's device by asking the device to 'forget' the wifi connection and password when disconnected. This means that the password needs to be input by the carer every time the child wishes to connect to the internet.

House rules

Have an open conversation with your family and the children in your care about appropriate internet use. A 2017 survey by the Royal Children's Hospital found that 94% of teenagers and 67% of primary-school aged children, along with 36% of preschoolers have their own device. Also 3 out of 4 teenagers and 1 in 6 primary school aged children have their own social media accounts.[1]

[1] The Royal Childrens Hospital publication; Australian Child Health Poll. *Screen Time and kids: What's happening in our homes?* https://www.childhealthpoll.org.au/wp-content/uploads/2017/06/ACHP-Poll7_Detailed-Report-June21.pdf

Carers should have regular open conversations with children about:

- Do not post your address, phone number or date of birth on your social networking page. Your friends should be able to ask you for this in person. Posting these details can open you up for stalkers, bullying, identity theft and online predators. This includes stating where you are when posting photos online in real time. There is no need for a child to be 'checked into' or geo-tagged at a specific venue or location on any social media account.
- Do not befriend everyone who sends you a Friend Request on social media. Be aware that you should only befriend people you know and trust in real life.
- Do not give your password to anyone. However, it *is* suitable for children to share their passwords with their carers, as part of their social media agreement.
- Do not send out pictures of yourself or others that show nudity or sexual acts. This is especially the case for children aged under 18. Children as young as 16 can be prosecuted for distribution of Child Pornography. This includes sending out a picture of someone else that was sent to you. If the pictures are posted online, it is impossible to completely remove these pictures from the internet. In extreme cases, photos of nudity can be reused on pornography websites around the world.
- Do not feel pressured to disclose your details to a stranger online. If your instincts tell you that something about the situation/person is not appropriate, then do not do it. Carers should have regular conversations with children about approaching carers if there is anyone who they feel is pressuring them to give out personal details. It is okay to say No.

- Be aware that what you post on the internet is there *permanently*, even if you think you have deleted it. Everything you do/write online is tracked and recorded. Things you write and pictures of yourself that are posted online can influence your ability to get a job in the future, as businesses can look online to determine what your personality is like. Carers should have regular conversations with the children in their care about this.
- Be kind online; do not bully others. Only say online what you would say if you knew your carer/parent were in the room with you.
- Use this guide to create a set of 'House Rules' for internet use. There is a printable version of house rules that can be found on page 10 in this manual.

Write up a house contract for internet use

Make a house contract with children. Make an agreement with them that:

- A general house rule is to not give out personal information online (such as full name, date of birth, address, phone numbers, school, local sporting club, passwords, etc) to anyone.
- Set specific times for when the internet is allowed to be used.
- They understand that people online are not always who they say they are.
- They should not meet a stranger they met online in person.
- The carers should agree to be available should the child experience difficulties online.

- That the child speaks to their carers immediately if they experience cyber bullying, or are made to feel uncomfortable in any conversations.
- Have a discussion regarding what constitutes an 'innapropriate' image. This includes nudity, gory imagery, bullying images, racism or sexism, or any other derogatory imagery.
- If required, write up a contract with the child, stating that they will abide by the above points. Have it in a visible area, such as the fridge.

Mobile phones

When giving a child a mobile phone, think about what type of phone/deal is appropriate for their developmental level.

See page 33 regarding making appropriate mobile phone choices for children/teenagers.

Some adolescents enter the foster care system with a mobile phone in their possession. Carers should utilise boundaries and create house rules that allow the child to use their phone and internet during set hours in the day. A common strategy is to ask an adolescent to leave their mobile phone in the kitchen overnight, to prevent them staying up late using their phone for calls/internet use.

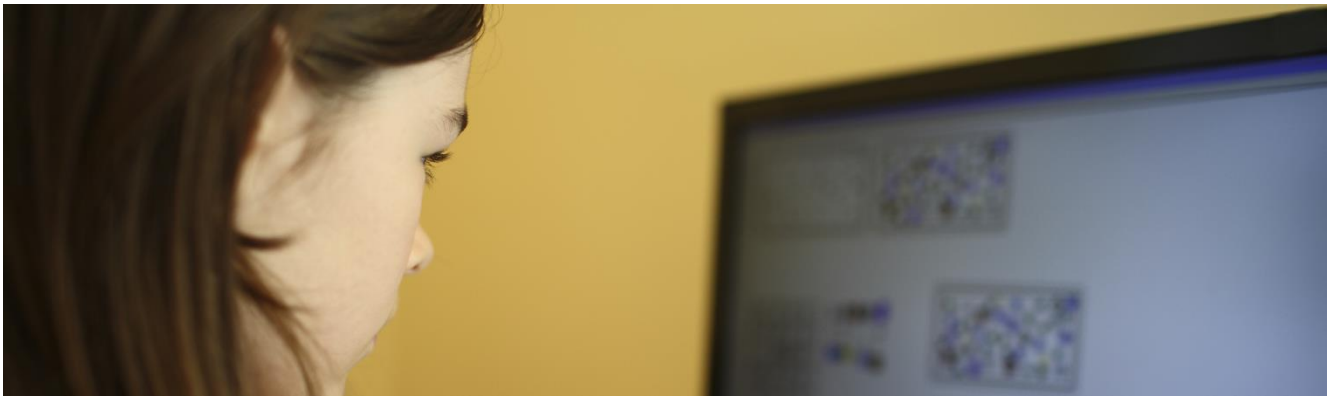
For mobile phone use regarding a foster child's contact with birth families and the child's safety, please consult your agency worker. Also see content found on page 285 in this manual for information about supervised phone/internet contact for children with their birth family members.

Device time limits and device locations

Keep devices in the living room or a public area in the home, when possible.
This is recommended for all homes, to be sure that the children are not engaging in deviant behaviour, and that the children can open discussions with their carers if they are being bullied or have someone initiating inappropriate conversations with them. Device/internet use is supposed to be a topic that can be discussed freely in the home. Secretive behaviour can indicate the child is embarrassed, engaging in inappropriate online behaviour or feeling victimised online. Carers should give the children freedom to use the internet, but ask them about their use. Be inquisitive and interested, but also be non-judgmental when speaking to the child about their internet use. Use strategies such as asking "Who do you talk to online? What are they like?", probing but not presenting

judgment. If carers then have concerns that arise when the child is discussing their online friends, then more in depth conversations can take place

Allot particular hours in the day for internet use. This also allows for more family face-to-face time. Carers can find that children can stay up late, using their Smart phones/laptops/tablets to connect to the internet from their bedrooms. If this occurs and the home has Wifi, a strategy could be unplugging the Wifi modem (even hiding the power cord) when everyone needs to sleep. If the home computer has the internet plugged into the modem with a cable, remove the cable. Or change the internet password so the child cannot log in when they are not allowed. Keep communication lines open so the children know that the internet will be reconnected in the morning and that this rule applies to all in the home. Alternatively, the use of a parental control program can limit the amount of time a child can spend online.



Parents and carers should take notice of their children's internet use

Parents and carers saying they are 'not tech-savvy' is no excuse to ignore the internet. If you do not know about social networking, ask the child and have the child show you how (for example) Facebook works while they are using it. The child may enjoy teaching you how to use social networking websites/apps. Be non-judgmental, but if you think something they are doing is not cyber-safe, create awareness with the child.

Make the Internet Fun

As a parent, carer, or worker it is your role to make the use of technology an enjoyable experience for the children in your care, but also making them aware of the dangers. Teaching children how to protect themselves is more useful than taking technology away from them. Use the internet together, exploring common interests (such as researching holiday destinations, or favourite movies).

Be aware of online scams

Be aware of online scams. Some emails that you receive can seem real and can trick you into giving out your passwords and other identifying information. See page 34 for more information on this.

Do not ban a child using devices or the internet

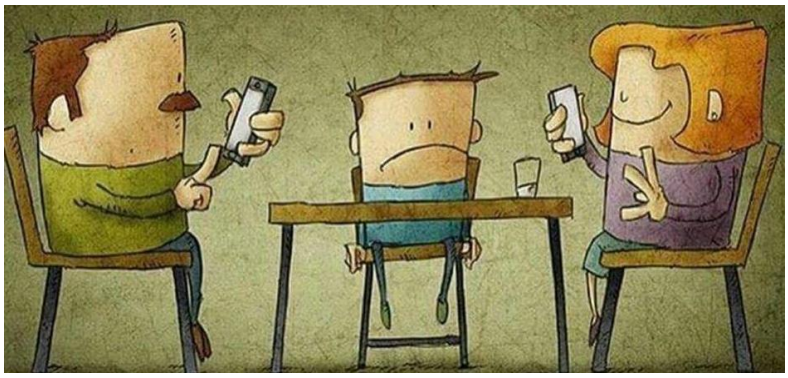
Smartphones and iPads/tablets are taking the place of family computers; giving children unsupervised and potentially unlimited access to the internet at all hours of the day/night. This is why education centred on how to surf the internet appropriately is so important. Building and maintaining trust between carer and child is paramount for cyber safety.

Children should be taught from a young age about appropriate internet/device use. Set time limits and maintain those boundaries. Banning a child or teenager from using the internet can at times cause the

child to use the internet in secret, such as using the internet at their friend's houses or at school. Internet use should be viewed positively within the home, as its use can be monitored appropriately within the home. Do not view the internet as bad. Instead look at addressing any concerning behaviours the child is exhibiting around internet use.
Allowing internet use at home will help a child to feel comfortable to speak to their carer, should any issues occur online.

Carers should also remember

- It is okay to say No. If a child wants a mobile phone/tablet device above their developmental need, then it is okay to say No, and maybe offer to review that discussion again in a year's time.
- Google yourself and family members regularly. Make a fun activity of it at least every six months.
- Regularly check the security settings on social media accounts. Do this check every 3-6 months for all social media accounts.
- You/Adults are the role models in the home. If you do not want children to use devices at the table, you also should not have your mobile at the table.



Please refer to the end of this booklet for glossaries on

- Computer and Internet terms (Page 40)
- Facebook and Social media terms (page 42)
- Internet Chat slang (Page 47)

Tips for Carers to Use When a Child First Enters the Home

For carers who take on new placements, it is important to explain the rules regarding internet/device use from day one.

House rules for internet and device usage need to be age-appropriate, and factoring in a child's developmental level. Some children are more mature than others, and some are more vulnerable than others.

House rules need to include:

- That an agreement must be made before the home wifi password is given out.
- Times of the day that the internet/devices can be used. It is okay to ask children to earn additional device/internet time in exchange for positive behaviours such as completing chores (eg. Setting the table, helping bring the shopping in from the car, offering to feed the pets, etc).
- In what rooms devices can be used (eg. Some carers prefer that iPads and phones are not used in children's bedrooms).
- Who in the home they should advise if their birth family makes contact with them online. (Carers should obtain information asap from their agency about any supervised and unsupervised access arrangements with a child's birth family or previous carers).
- What websites and content are appropriate to be accessed, along with which are not allowed to be used. Make a list of appropriate websites that the child can access, including social media apps. Make time to sit with the child and compile the list together, and make time to review that list on an ongoing basis.
- Who has access to the password for their social media accounts, along with why children need to share passwords with their carers. Carers need to be clear that it's purely to check their messages are not unsafe, and that carers will not be impersonating the child online.
- Have a discussion with the child, advising them that the adults at home are available to help at any time if the child comes across any content that is innapropriate, or if they're subjected to bullying, predatory behaviour or unsure of how to approach a social situation online.

On the following page is an example of a contract carers can use with children. This should also include usage times for devices such as game systems (such as PlayStation and Xbox).

Printout for carers to use in the home:

House Rules – For Internet Use:

If you don't know the person in real life, then they are a stranger.

NEVER GIVE A STRANGER YOUR FULL NAME, PHONE NUMBER, PASSWORDS OR ADDRESS.

If you are being bullied, or know someone being bullied, you need to tell:

_____

Internet time each day starts at: _____ And ends at : _____

You can use the internet in these rooms of the house, where grown-ups are around to help you:

_____

If these people try to contact me online:

_____

Then I will tell _____ about it.

Other rules in our home for using the internet and devices:

_____

_____

_____

_____

Social Networking Websites, Apps and Programs

There are a large number of social interaction websites and apps (applications).
Here are a small number of the popular programs/websites used by adults and adolescents.

Deviant Art
This is a website dedicated to art. Users are able to create an account and post their artistic talents online. Parents and carers need to be aware that content is not censored if users make an account and log in. It is an artistic website, so there is some nudity, which is automatically blocked from view if users don't log into an account. www.deviantart.com

Facebook
Facebook is the most popular of the social networking websites. It operates in a way that allows users to make a profile page, and become 'friends' with others, sharing photos, status updates (short sentences describing how they are), videos, etc. www.facebook.com

Facebook Messenger
This is the application created to allow Facebook users to send private messages to one another. It also allows users to send photos, videos and text to selected persons without the content appearing on the user's Facebook profile. It is commonly used as a smart phone app.

Facetime
Facetime is a video chat application developed by Apple, available for Apple users only (eg. Apple iPhone to Apple iPad). It operates like a video conference call, however uses the phone's Wifi/internet usage to operate for free.

Fortnite
A video game, gaining fast popularity in 2018 with primary and high school aged children. It is a game where children can pick what they want their shooter avatar to look like, as they run around an island, shooting others. This game is known for not having blood splattering and looks more cartoon-ish, which is partly why it has gained the popularity and idea that it's a shooting game for primary school-aged children. It has features that allow children to play against other people online, including using headsets to speak to and hear others. Carers need to be aware that there is no filter regarding the type of language others may be using when using the headsets. Children will need to pay for upgrades, with credits called 'V-Bucks'. So please be aware if you have a credit card attached to the account they are playing from.

The maturity of the child should be taken into consideration with regards to if they should play this game or not. Conversations should be had with all children about socialising with strangers online, along with the knowledge that language is not filtered. People of all ages play this game, and children will be exposed to swearing and insults from others. It would be preferable that children play without

the headsets. It is highly recommended that time limits are also put into place, as carers have found children become addicted to videogames like this.
An article about things that carers need to know about Fortnite;
https://www.tomsguide.com/us/fortnite-parents-guide,review-5552.html
Also refer to *Online Gaming* further down on this page.

Flikr
A website designed for sharing photos, used particularly for those passionate about photography.
https://www.flickr.com

Hangouts
Google Android's version of iPhone's Facetime, and Facebook's Messenger app. It is an app on android phones that lets users connect to each other by their Gmail accounts. They can send messages, photo and video chat via Wifi or internet. This comes pre-loaded on most Android phones/tablets.

Habbo
Habbo is a chat program which is aimed at use by children and teens. However it is also at risk of adults finding ways to get online to chat to children. There are moderators, whose job it is to remove inappropriate users, but this does take time after a user joins the forum, and so there is still risk involved. https://www.habbo.com/

Hotel Hideaway
Similar to Habbo, this is another chat program aimed at children and adolescents. Avatars can be designed and go into different rooms/environments to chat. Carers need to be aware that characters have been noted to imitate sexual advances and gyrating. This game should not be used by primary school aged children. https://www.hotelhideawaythegame.com/

Instagram
A form of social networking that allows users to follow one another through photos. Photos can be linked to social networking sites such as Facebook and Twitter, where the photos can also appear. Users need to be aware that while the etiquette on Facebook is that you add friends who you know in real life, on Instagram, profile pages are automatically open for public viewing, and strangers will often 'Follow' each other's pages. Parents and carers are encouraged to ensure children have their profile pages locked, and they approve who can see their profile content. On Instagram it is possible to follow someone without the other person seeing your page. Instagram is popular with celebrities; sharing photos with minimal communication from fans. https://www.instagram.com/

Kik Messenger
Kik is advertised as a *free texting app* for smart phones. This app requires users to create a username, which is what's used to connect with others. It also allows for users to chat to strangers who also have the app. This app has received criticism due to this feature, as children need to be aware of the dangers of speaking to strangers online. Also some can receive messages from random users who guessed their username. https://www.kik.com/

Myspace
A social networking site dedicated to those who wish to share and promote musical talents. It also allows users to blog, add photos and videos. It now offers forums, where groups of people with similar interests can converse. https://myspace.com/

Online Gaming
It is also worth noting that online video gaming is a great way for children and adolescents to interact with their friends online. It offers an opportunity for them to play, while being able to speak to their friends (often through use of a headset) if they cannot sit with their friends in the real world. However it also opens up cyber safety issues, predominantly relating to predators using it as an avenue to make contact with children online, or children being exposed to bullying online. The links provided are great resource for safe online gaming guidelines for children.
Office of the eSafety Commissioner: Online Gaming https://esafety.gov.au/esafety-information/esafety-issues/online-gaming

Onlingg gaming: An introduction for parents and carers: https://www.childnet.com/ufiles/Online-gaming-an-introduction-for-parents-and-carers-2017.pdf

Pinterest
This is a virtual pinboard where users can post photos, recipes and share ideas. Users can browse pinboards created by other people around the world and comment on them.
https://www.pinterest.com.au/

Skype
Skype allows users to make video and audio-only calls to others. It can be used to contact other members who also use the program or with credit purchased, it can be used to make discounted calls to phones. http://www.skype.com/en/

Snap Chat
This is an app that allows users to send photos to one another, however the image disappears after 1-10 seconds (depending how long the sender chooses the photo to appear for). This operates using the user's phone and contact list to send images. Snap Chat has received criticism over the years as it can be used by some to send sexually explicit images (such as sexting). With changes in technology, and the ability to 'print screen' (copying the image on the screen), images can now be copied and continue to be distributed. Snapchat also alerts the original sender if someone else printscreens their photo. Snapchat also allows for written messages to also be sent via this application. https://www.snapchat.com/l/en-gb/

Spectacles are sunglasses released in conjunction with Snapchat. They have cameras on them, to allow users to take photos as they go about their day. Concerns with this is it that others can be filmed & photographed without permission.
https://www.spectacles.com/

Spotafriend
On the Spotafriend website, it advertises *Meet teens near you with Spotafriend, a Tinder alternative for people ages 13-19.* However, the website claims that it is not a dating service, but designed for teenagers to find friends. This website has similar traits to Tinder, which is a popular online dating app. Spotafriend has been slammed by parent groups and the media, reportedly due to paedophiles specifically using this app to speak to children. With the reference to Tinder, it also creates the impression for youth that they could use the app for "hook-ups" with other children their age. The website boasts being an app to help children make friends, but the website has blogs relating to dating turn-offs, and dating tips. It also allows users to sort their search by Nearest youth, Newest youth, Popular and Hottest. https://www.spotafriend.co/

TikTok (formerly known as Musical.ly)
The official TikTok website states; *TikTok is a destination for short-form mobile videos. Our mission is to capture and present the world's creativity, knowledge, and precious life moments, directly from the mobile phone. TikTok enables everyone to be a creator, and encourages users to share their passion and creative expression through their videos.*
Although the app promotes creativity, some concerns have been raised by carers and parents alike, on the risks for children using this application. The app gives users the ability to chat to strangers online and send instantaneous pictures/videos. This has caused issues whereby predators online have used the app to groom children and send/receive pornography, especially using hashtags/names of files that seem innocent to attach their pornographic content to.
https://www.tiktok.com/

Tinder
Tinder, is a popular online dating app for adults. It uses the GPS feature on users phones, to show dating matches with adults in a similar geographical area. It also will not work unless a user logs into it using their Facebook account. The rationale behind this for Tinder is that it will use the shows/hobbies/pages a user has liked to match with people who have similarities on their Facebook pages. Tinder also has negative connotations that it is an ideal meeting site for one-night-stands, and encouraging people to meet strangers they met online. Tinder should not be used by children or adolescents.
https://tinder.com/

Tumblr
This is a virtual pin board that allows users to share photos, art, text, music and videos online. The Tumblr website advertises *We made it really, really simple for people to make a blog and put whatever they want on it. Stories, photos, GIFs, TV shows, links, quips, dumb jokes, smart jokes, Spotify tracks, mp3s, videos, fashion, art, deep stuff.* https://www.tumblr.com/

Twitter
Twitter operates in a manner that lets users write only short sentences about what they are thinking. These are called Tweets. Photos can also be posted online. Like Instagram, Twitter is an application that allows users to 'Follow' others and see their content, without the other person having to follow them back. Whatever tweets and photos are shared, are visible by anyone around the world. There's no setting to lock one's page. All pages and accounts are public to the world. Users tend to use Hashtags, which can be searched by anyone across the globe.
https://twitter.com/

Youtube
Youtube is a video-sharing website on which users can upload, share, and view videos. This can include video diaries. Although parents and carers allow their children to watch cartoons from Youtube, it is highly encouraged that a child's usage is monitored. For example, in 2016, there was controversy around Peppa Pig videos which were changed, to feature gory imagery and inappropriate language, then uploaded to Youtube . https://www.youtube.com/

WhatsApp
WhatsApp is another application, similar to Skype. It allows users with the app to send messages and make calls to one another, on mobile phones and tablets, using internet data. Whatsapp also links the account to a person's phone number. https://www.whatsapp.com/

Whisper
Whisper is a page whereby youth and adults can share their deepest darkest secrets anonymously. The page has now expanded, showing 'Top 10 confessions', themes, and shares its content on other media such as Facebook and Twitter. http://whisper.sh/

Yubo (formerly known as Yellow)
Yubo is an app that allows Snapchat and Instagram users to *make new friends and spend time with them with chat and live videos*. This app has been described on social media blogs as an alternative to Tinder, asking users to list their preference for meeting males or females, what their location is, and their date of birth. The app offers a similar 'swipe right', 'swipe left' feature that Tinder offers. As with the previously mentioned apps, parents and carers should discuss the risks when meeting strangers online with the children in their care.
https://www.yellw.co/ Also, Yubo offers a cyber safety flyer for adolescents http://teens.yubo.live/

This is just a small representation of the social networking sites out there.
More are popping up every day.

Regardless which social media app/website you or the children in you care use, it is important to familiarise yourself with the general cyber safety tips in this manual.

This includes having open conversations with children in your care, being aware of the content they are viewing online, and educating them on online safety.

The eSafety Commissioner has further information about a large range of social media apps and websites.
https://www.esafety.gov.au/esafety-information/games-apps-and-social-networking

Child-Orientated Websites

The following programs, apps and websites are aimed for use by predominantly primary-school aged children.

Some of these websites are monitored 24-hours per day for inappropriate language (such as swearing and sexual content) and can provide educational components. Some of these websites require a paid membership.

Parents should still educate the children in their care about cyber safety, and set rules, such as avoiding giving out their phone numbers, passwords and personal details to strangers on these websites.

Club Penguin
A social website aimed at children 6-14 years of age It is moderated for inappropriate content, and aims to be a safe place for children to play online.
https://www.clubpenguinisland.com/

Kiddle- A Safe Visual Search Engine for Kids
A child-friendly search engine, powered by Google. It has filtered out any searches that are deemed inappropriate to children. https://www.kiddle.co/
More information about this search engine can be found here: https://www.kiddle.co/about.php

Moshi Monsters
Children create their own pet Monster. An educational networking game for kids of all ages.
www.moshimonsters.com

Minecraft
A game where children can create their own world by building/digging, creating lands with the use of 3D blocks. However the game is only cyber safe during single-player mode. There is the capability for children to play multiplayer mode, which invites other online users from the public to step into the child's 'World'. Unless the child knows who the additional players are, multiplayer mode is not advisable. Although Minecraft is considered as a 'child friendly' game, it is not monitored for inappropriate behaviour. https://minecraft.net/en-us/

Poptropica
A virtual world which requires children to complete tasks and socialise with others.
http://www.poptropica.com/

Roblox
Roblox states on its website that *Roblox is the best place to imagine with friends*. It advertises that it is similar to that of Minecraft, however it has come under scrutiny recently, with reports that paedophiles have hacked into the software, using their avatars to simulate sexual intercourse with the

avatar children are using, in an attempt to groom them. Parents and carers are highly advised to carefully monitor a child's play with this game. https://www.roblox.com/

Undertale
Undertale is a pixelated role playing game, which is advertised to be child friendly. The website advertises that it is *The friendly RPG (Role-Playing Game) where nobody has to die*. The main character is a child, who needs to complete tasks to progress through the story. The game can be played on Mac or PC, but requires purchase. https://undertale.com/

It is understandable that a parent or carer will feel overwhelmed with the number of dangers there are for children online.
However, there are many websites that offer advice and support to parents and carers.

One example can be found at:

Common Sense Media
This website advertises that they have reviews for parents about movies out in cinemas, TV shows, books, websites and games.
Their website states: *Achieving a healthy approach to media and technology can make a big difference in kids' lives today. Kids who learn to use digital media wisely can accomplish amazing things — learn new skills, explore new worlds, build new ideas, and change the world. Yet every kid has different needs. As parents and educators, we know our kids best. Common Sense is here to help. We can steer you away from things that are developmentally inappropriate, and help you find the hidden gems that are right for your family and your kids*
https://www.commonsensemedia.org/

Facebook risks:

Who can see what you write?

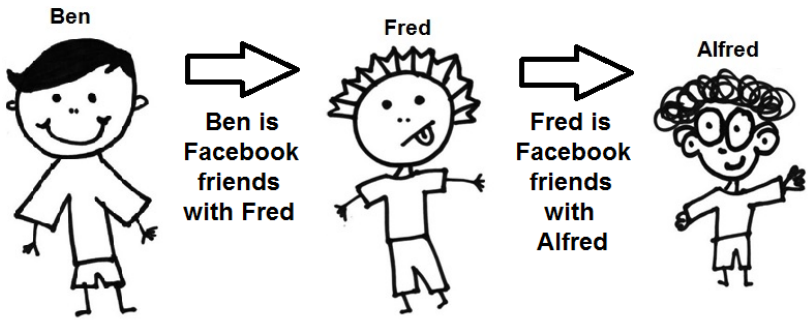
Facebook is one of the most popular social networking websites available across the globe.

Everything you post (status updates, photos, etc) will appear on your profile page. So if Facebook friends go onto your profile page then they will see your online activity. It is important to keep your profile set so that your photos and personal information can be seen by your *Friends only*. This is a rule that families should be encouraged to use with all their social media pages.

Facebook users need to remember who they are friends with when they post comments.

One issue that Facebook users tend to forget, especially when writing comments, is sometimes people who are *friends of your Facebook friends* can sometimes see your messages, posts and photos on Facebook.

An example of how this works:
You are Ben. Ben is Facebook friends with Fred. Fred is friends with Alfred. Alfred normally has no direct contact with Ben, because they are not Facebook friends.



Ben writes a status update on his own wall, stating: *Had an awesome night out, but that Alfred guy was really annoying!*

At the moment, Alfred cannot see this status because Ben is not friends with Alfred. Also, Ben assumes that Alfred will not see it. Fred can see the status, because he is friends with Ben.

Fred adds a comment to Ben's status, stating: *It was such a great boys night out! We need to catch up again!*

Because Alfred is friends with Fred, Alfred can sometimes see what messages Fred is writing.

This gives Alfred access to the message Fred wrote on the end of Ben's comment. So Alfred can now also see that Ben thinks he's 'annoying'.

This situation can cause issues regarding to social etiquette and confidentiality for carers, children and workers. This can include the following examples:

Foster carers who speak about fostering/workers/agency issues on social media. There is more information regarding this on page 26, regarding etiquette for carers to use on social media.

Social workers who speak about work/client issues on social media. All agencies should have a social media policy for staff regarding representing their place of work online. Also about confidentiality; not disclosing client information on social media.

Children in care who are unaware of conflicts that could occur in real life due to comments made on social media. For example, a child who makes comments about a fellow student online, not realising the repercussions could result in an argument with another student at school the next day.

. Online Grooming

It is important to be aware that the internet is a great method of communication that is used by a wide range of people all over the world. While it is convenient, online communication also carries risks.

Online grooming occurs when someone initiates contact with a child with the intention of preparing them for sexual abuse online or in the real world.

Online grooming is illegal.

Essentially, the grooming process is gradual, where groomers will introduce sexual conduct into conversations, in a way of preparing the child so that they can begin to sexually abuse them later.

Online groomers can operate by:

- Befriending the child online. They can tend to pretend to be similar age to the child.
- Gaining the child's confidence by offering to be a sympathetic ear, listening to their problems and giving them lots of positive attention.
- Gathering the child's personal details (name, what suburb they live in, what school they attend) so they can manipulate the child into meeting them in real life.
- They can begin as a 'friend' and then later turn into a bully to gain control over the child, as a way of forcing them to send sexualised photos of themselves or meeting in real life.
- Building the child's trust, then changing the topics of conversation to a more sexual nature.
- Breaking down the bonds between the child and their parents. Therefore convincing the child that their parents do not understand the child, and that the predator understands them instead.
- Asking the child to send photos of themselves that are sexual in nature. Predators can be known to distribute these photos to other predators, or use the photos to threaten the child into sending more photos of themselves.
- Exposing their own genitals to the child via photos or a webcam.
- Sending the child presents in the mail, including paying for a child's mobile phone credit or providing them with transport tickets to bribe the child to meet with them in person.
- Asking the child to meet them in real life, with the intention of sexually abusing the child.

To make a complaint about online child sexual content, or to find out more, please make contact with the Office of the eSafety Commissioner at https://esafety.gov.au/complaints-and-reporting/offensive-and-illegal-content-complaints/the-action-we-take

Possible signs that a child has been targeted:

- Your child is becoming withdrawn, depressed and displaying behavioural changes.
- You find pornography on your child's computer.
- Your child is spending large amounts of time on the internet.
- When you enter the room, the child quickly changes the content on the screen, or turns it off.
- Your child is receiving gifts in the mail from people you do not know.

Important things to remember for parents, carers and children:

- If you are speaking to someone online that you have not met in person, do not give them any identifying information, such as where you live, phone numbers, email addresses, and so on.
- Do not send out images of yourself to others online that are sexual in nature, such as naked pictures or even videos conducting sexual acts.
- Be aware that not everyone online is who they say they are. Do not tell strangers what suburb you live in. A general rule to use: If you would not tell a stranger in person, do not tell them online. For children in care who have indisccriminant behaviour, please use ongoing reminders of this fact.
- Do not meet people that you met online. If you do, make sure it is a well-lit, public place where other people can see you and the person you are meeting. Always let someone know where you are going to be and what time you are due back, in case something happens to you. This should be a general rule for adults too (eg. if meeting someone to pickup an item purchased online).
- Parents and children should have regular conversations about the people that children are speaking to online. Make the child aware of the dangers. Even though conversations on the topic of sex can be embarrassing for children, it is important that they tell their parents or carers when someone has been speaking to them about it online. Carers can use strategies when speaking to children that present as non-judgemental, to help the child feel that they can open up. Eg. "Who did you meet online today? Are they nice? Tell me a bit about them. What do you guys talk about?".
- Children are now more likely to meet a sex offender online than in real life.
- Online predators have a higher chance of meeting children online during the school holidays, when children tend to spend more time at home on the computer.
- Online grooming can occur to both boys and girls.
- Online grooming can begin through a range of platforms, such as social networking websites, chat sites/apps and online gaming.

What to do if you believe a predator has made contact with a child in your care:

If you believe that the child is in immediate danger, call the police on 000.
Otherwise, you can contact the Australian branch of the Virtual Global Taskforce (via the Australian Federal Police) at https://forms.afp.gov.au/online_forms/ocset_form and fill out an Online Child Sex Exploitation Report Form. They will then investigate the matter further.

Cyber Bullying

Cyber bullying is the act of bullying others through the use of technology (computer, text messages, emails, phone calls, internet chat, social networking websites, and so on).

Cyber bullying is characterised by the fact that victims can be reached anytime and anyplace, while bullying in the real world occurs in social situations, such as at school and work.

Cyber bullying causes victims to feel shame, embarrassment, anger, depression, experience withdrawal and fear, and have high anxiety. Victims can tend to have poor assertive skills, have difficulties at school, and have fewer friends.

Cyber bulling has become a major issue in society. It is important for parents to educate their children about how harmful cyber bullying is. Extreme cases of cyber bullying have resulted in victims committing suicide. Cyber bullies do not really understand or empathise with how harmful their comments are because they cannot physically see their victims, and these bullies feel more confident to comment from the safety of their keyboard.

There are several types of cyber bullying:

- Stealing people's passwords and accessing their account, then impersonating them.
- Sending harassing pictures through text messages, email and social networking websites
- Sending pornographic images or spam.
- Sending harassing and threatening comments through instant/text messaging and social networking websites.
- Sending threats to harm others or their possessions.

There are a number of types of cyber bullies:

- Bullies who do not realise they are bullies. They become bullies themselves when they retaliate, thinking they are protecting the victim.
- Bullies that require an audience when bullying others. Afterwards they often brag about what they have done. Bragging can be in person, with screenshots (evidence), or bullying is done in a public forum online
- Girls who build their own ego by bullying others. They bully as a way of entertaining themselves. They often operate in packs, with a number of them bullying a single individual.
- Inadvertent bullies, who do not think they are bullies. These bullies are angry and send hurtful comments without thinking of the consequences.
- Trolls are people who bully online by deliberately sending hateful messages, often to strangers.

What to teach children if they are being cyber-bullied

- Never retaliate. Do not respond to messages when you are angry or hurt. Bullies feed off your reaction. This will often encourage them to continue or increase their harassment. Log out and stop messaging if you feel you are being harassed.
- Tell an adult you trust. You do not need to suffer the taunts of bullies alone. Tell someone what's going on so they can help you deal with the situation.
- Keep a record of abusive messages, calls, posts and emails that may be hurtful or harmful to you. Record everything you can to give to the authorities at a later date. You can also do this by using the 'Print screen' button on the computer or phone. On the computer, the image can then be pasted into a Word document.
- Remember you have the option to block, delete and report anyone who is harassing you online and on your mobile. Most social media apps have a 'report' button for these instances. Do not be afraid to use these features if you are experiencing harassment.
- Find any personal information you can about the bully. Consider using this information to contact their school, employer, or if necessary, the police or eSafety Comissioner.

Consult with the child's school for peer bullying, or the police in extreme cases. Parents and carers are encouraged to remind children that it's safe to approach them if they're being bullied.

Asking children to simply 'ignore it' and turn off their phones will not always solve the problem. Carers need to make children feel they can talk to the adults around them about these issues, without judgement. It is important for parents to educate their children about understanding how this is not an appropriate way for children to communicate with one other.

Resources:

The ReachOut website for strategies:
https://au.reachout.com/articles/5-strategies-for-dealing-with-cyberbullying

The eSafety Commissioner website on reporting on Cyber Bullying:
https://esafety.gov.au/complaints-and-reporting/cyberbullying-complaints

Wired Safety – An American educational tool on cyber safety, sexting, cyber bullying, cyber stalking, etc. https://www.wiredsafety.com/

eSafety Homepage- (previously named Cyber Smart).
An Australian Government Initiative, run by the Office of the Children's eSafety Commissioner. The website aims at teaching and providing information for children and parents about cyber safety.
To report issues on Cyber Bullying and Illegal content online, please refer to:
https://esafety.gov.au/complaints-and-reporting/offensive-and-illegal-content-complaints/report-offensive-or-illegal-content

Sexting

What is it, and why are adolescents doing it?

Sexting is the term given when someone sends pictures, messages or videos to another, with the subject provocative, sexual, or showing explicit nudity. The name comes from combining “sexy” and “text”. It has become an increasingly contentious issue amongst adolescents, who sometimes don’t comprehend the damage that sexting can do to their reputations in adulthood.

Why adolescents may sext one another:

Why some send sexts to others:

- Because (predominantly) girls feel it’s expected of them, or else they could be called a ‘prude’.
- To receive more attention from someone they feel attracted to, to feel ‘sexy’, and flirt with others.
- To receive positive feedback from their peers (this includes getting more ‘likes’ on social media, more followers, and being told they’re sexy).
- Because they feel pressured by others.
- To feel the rush of doing something ‘risky’.

Why some ask for sexts from others:

- Because (predominantly boys) feel it’s normal to ask girls for nude pictures.
- To forward the pictures to their friends (whether it’s to feel cool to bully or get back at the person sending the sext).
- They have a lack of education about respect for the opposite sex/ lack of education about respect for others (this relates more to those who ‘rate’ or purposely share the pictures with others).

What damage can sexting do?

- Distributing photos can damage that person’s online reputation. If photos are posted online, they are there to stay. Websites may be able to offer the option of deleting photos, but all information posted on the internet is saved to servers, which means photos can still be retrieved, saved and distributed by others.
- Apps such as Snapchat, which adolescents may use because the images ‘disappear’ after a certain number of seconds, do not guarantee that the images can’t be copied (or print-screened) in the process. Then photos can continue to be shared/kept by others.
- Pictures can be shared across the globe and be used on pornography websites. From there it is impossible to have the photos/videos removed.
- Inappropriately sharing images/videos of others of a sexual nature, without their consent can result in criminal charges. If the subject is underage, then additional child sex offences can occur to those distributing the content.

Legal Ramifications for Sexting

If someone has a nude picture on their phone, laptop, tablet, etc of someone under 18 years old, they can be charged for possessing child pornography. If you then send the photo to someone else, you could also be charged. As of November 2014, laws were changed to prevent children being placed on the sex offender registry or have a criminal record. The new laws prevent children from being inappropriately prosecuted. For the full media release, please refer to the *Additional Government Resources* pages towards the end of this manual.

Some tip sheets have been created by the Centre Against Sexual Assault (CASA), which have practical solutions for children and families to use to protect a child's online identity, protect from sexual exploitation and how to respect others online.

These sheets can be found at: https://esafety.secasa.com.au/grown-ups/resources/

What is image- based abuse?

Image-Based Abuse (IBA) occurs when someone else shares a picture of you that is intimate, has nudity or genitalia showing. Threatening to share those images is also classed as 'Revenge Porn'. This also includes any photos that are photoshopped, and includes the threat of photos being shared without consent.

Sadly, 1 in 5 have experienced IBA and women aged 18-24 are more likely to have it occur to them.

For more information, or to report Image-based abuse visit
https://www.esafety.gov.au/image-based-abuse/

In 2018 Supre, in partnership with the Alannah & Madeline Foundation, released a set of booklets aimed towards teenage girls (but boys would benefit from reading them too). They are available for free download:

Bullying. So Not Okay. https://supre.com.au/on/demandware.static/-/Library-Sites-supre-shared-library/default/dw96d14216/Supre/2018/4_PDF/FoundationAntiBullyingBooklet.pdf
or https://headspace.org.au/assets/Uploads/Bullying-So-not-Ok-Booklet.pdf

Image Based Bullying. So Not Okay https://supre.com.au/on/demandware.static/-/Library-Sites-supre-shared-library/default/dw393a91d8/Supre/2018/4_PDF/Image-Based-Bullying-So-not-OK.pdf

Other Sexting Resources

Kids Helpline Sexting factsheet. https://kidshelpline.com.au/teens/tips/sexting-and-the-consequences/

The Line: http://www.theline.org.au

The Office of the eSafety Commissioner: Sexting

https://www.esafety.gov.au/esafety-information/esafety-issues/sexting

Lawstuff: know your rights http://www.lawstuff.org.au/vic_law/topics

Specifically legal information about sexting in Victoria, Australia

http://www.lawstuff.org.au/vic_law/topics/Sexting

General Guidelines for Carers on Social Media

There are a large number of foster care forums, and groups on social media.

Although it would appear common sense, here are some guidelines for carers to abide by when speaking about caring and fostering online.

Be aware that with these guidelines, there are a number of private online forums (such as locked Facebook groups), that only allow the members (rather than the general public) to see messages posted on them. Carers can feel a sense of connection to other carers via forums or groups. Carers may also feel that they can then speak more freely about grievances and more honestly about their opinions on matters relating to the foster care system.

However, carers need to be aware that even if the forum is locked:

- Carers should not name their foster child, or give identifying information such as school details or address locations. Carers need to be cautious about also disclosing specifics of a child's trauma and medical history as it could also be classed as identifying information.

- Photos of children under court orders should not be posted in forums related to foster/kinship care. Even if the forum appears to be locked to carers only. Carers need to be aware that although the forum may be locked to members only, there are no guarantees that the privacy settings of the other members will be adequate to maintain the child's privacy.

- If other forum members have concerns about a carer's wellbeing, conduct or language when describing the child/birth family, or have concerns about breaching general confidentiality, they can report that to the foster/kinship care agency/Child Protection service in your area.

- Children are able to have their photos posted in school publications, and even appear in the newspaper (such as a good-news article), provided they are not labelled as a child under a court order. *[This is a guideline that the Department of Health and Human Services Child Protection in Melbourne have advised. Please check with your local child protection agency for legalities in your area].* However, for example, posting photos of a foster child in a foster care forum, even without labelling who is a foster child can still label that child. Carers need to be aware of the difference. Please consult with your allocated agency for more information about this.

There are potential legal issues that carers may face if they are caught indicating on social media that a child is under a court order. Please see **page 39** for more information on the handout from the Department of Health and Human Services Child Protection in Melbourne. Also please consult with your agency for the legalities of this in your area.

If you want to boast about your foster child(ren)'s achievements on social media to your friends/other carers:

DO:

- Refer to the child by code names such as "My little one", "Miss 9yo" or "Mr 2yo".
- Remember who you are friends with on Facebook. Are there any friends of your friends who know the child's birth family?
- Give photos captions such as "Our family day out" rather than "Day out with our foster children".

DON'T:

- Give identifying information that discloses that they are a child under a court order. This also applies to filtering and deleting any comments made by others on your posts that identify the child as being on a court order.
- Use the children's full names.
- Give information that identifies the child's school, case plan, identifiable medical issues, supervised contact conditions, etc.

If you have an issue with your care agency/Child Protection/Court outcome, or have concerns around the child's contact arrangements/birth parents:

DO:

- Debrief with your allocated worker (or a duty worker) at your care agency.
- Debrief with other carers privately, in person or on the phone.
- Discuss your grievances with representatives of the FCAV (Foster Care Association of Victoria), or Foster Care support network in your area.

DON'T:

- Complain publically on social media.
- Name and shame workers, the agency/issue or parents/system online.
- Name the child, or give any information that identifies the child as being on a court order.

More information can be found on the Foster Care Association of Victoria Website:

Good Practice on Social Media Guidelines
https://www.fcav.org.au/images/carer-resources/information-sheets/Good_Social_Media_Practice.pdf

Photos and Social Media Guidelines
https://www.fcav.org.au/images/carer-resources/information-sheets/Good_Social_Media_Practice.pdf

Even though workers, carers and children work together, befriending them on social media blurs worker-client boundaries. As a general rule,carers and children should not befriend their workers, and vice versa. Sometimes when a child has left their care, carers need to be aware that sometimes it is not appopriate to befriend these foster children online. Many carers wish to remain available to support the child if they need. There are positives and negatives to this, so carers should consult their workers if they are unsure.

Children in Care and Supervised Contact Arrangements

Children in care are subjected to Children's Court Orders, which often come with court ordered conditions. This, at times, includes children requiring supervised contact (also known as "access") with their birth parents/family.

Please note: As of March 2016, case planners at the Department of Health and Human Services Child Protection in Melbourne have the power to dictate access conditions for children on court orders to Out Of Home Care (OOHC, aka Foster Care or Kinship Care).

It is important to note that if the court order and Child Protection stipulate that contact needs to be supervised, it doesn't just apply to face-to-face contact. This also applies to contact that occurs on the phone, or even online.

Examples of access conditions can include wording such as:

> Mother may have contact with the child at times and places as agreed between the parties. DHHS or its nominee will supervise contact unless DHHS assesses that supervision is not necessary. Contact is subject to the child's wishes.
>
> Father may have contact with the child once per fortnight for 3 hours on weekends at times and places agreed between the child, the father and DHHS. DHS will monitor the contact unless DHHS assesses that monitoring is no longer necessary. Contact will not take place if the child does not wish to attend.

If a parent or birth family must have supervised contact, then it is important for the child to also be made aware of this.

There have been instances of parents or birth families making contact with children through social media, and children not being aware that they need to have this contact monitored.

If carers find that contact online or via phone is occurring between their child and parent (which should be supervised), please speak to your allocated worker. Carers should also have conversations with the child in their care about keeping open conversations about if their family are making contact with them.

If the parent or birth family prefer contact to occur online, (whether it be through chat, via text only, video call or audio only) then this needs to be discussed first with the Child Protection and agency workers.

If it is deemed to be an appropriate method of communication between the child and parent, then plans need to be made around:

- Who will be supervising this contact? Contact online would generally occur when the child is at home, so supervision in this case would likely fall upon the carer. Carers can advise their workers if they do not feel comfortable supervising contact.

- When will this supervised contact be scheduled to occur? If there is video-chat, phone calls, or instantaneous chat via a messenger service, then it would be preferable to set a time/day that this occurs. This allows carers to be present should the parent/birth family speak about content that is not appropriate. If need be, ask your agency worker to send a set schedule with dates/times to the birth family.

- If contact occurs outside of the pre-arranged agreement, the child should notify their carer and worker in a timely manner.

- Carers should have a discussion with the child before access occurs. This includes whether the carer will need to sit with the child or not, appropriate topics of discussion (especially if children struggle to maintain conversation for long), and not contacting their parents outside these arranged dates/times.

Carers should have a plan when supervising access, in regards to devices used. This can include:

- For phone contact, use a cheap basic mobile phone with a separate simcard, turned on only when access is due to occur. Then the phone can be turned off between contacts (The birth parents should also be made aware of this fact). Otherwise set your phone to dial out with a private number. A separate smartphone is also an alternative, especially if apps need to be used, for contact via wifi. The phone can then also be turned off around accesses.

- Using a set device or a separate account for any apps that can call parents via Wifi. Using a different device altogether means that carers don't have to worry about constantly logging in and out.

- Talking to the child about who in the home or care team knows and controls the log in details for the app used to contact the parents with.

GPS Tracking and Safety

Apps on mobile phones are one by one tracking the geographical location of their users.

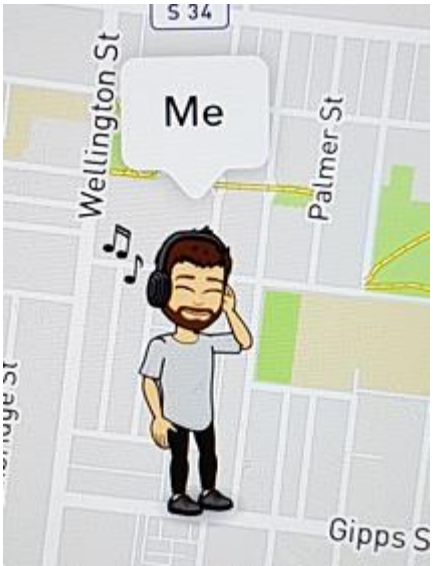
This can occur when mobile phone users

- Leave the GPS feature on their phone turned on at all times
- Forget to turn the GPS off
- Haven't adjusted privacy settings on social media
- Haven't kept up to date with ongoing changes in privacy settings on social media.

Examples of this include

- *Facebook*: In recent years, there have been incidents whereby Facebook has shown the suburb that people are in when posting status updates.
  Also previously Facebook Messenger showed the location users were from, down to the street and house number, when they sent private messages from their phones.

- *Snapchat*: A 2017 Snapchat update created a map that allowed others to see where people are (pictured right). This also showed where users were, down to the street and house number. The added issues around this, is that Snapchat also showed what users were doing, such as listening to music on their phones (pictured below), or travelling in a car. To turn off this feature, Snapchat needs to have 'Ghost Mode' turned on.



It is important for carers, and all family members, to regularly (at least every 6 months) review the privacy settings on their social media apps. Even if the privacy settings were set up when the social media account was initially created, updates to the apps can at times return privacy settings to the default. This means that there is a chance that content can be seen by those around the world.

All household members should be encouraged to adjust the social media privacy settings and ensure that their pictures, personal accounts and location can only be visible to friends only. Children still need to be aware of who they are friends with on social media, and consequently who can see their location.

Ideally, children should be encouraged to have the GPS location in social media apps turned off at all times. However, there are issues that can arise with regards to children in care, whereby some chronically abscond, and need workers and carers to locate them for safety reasons. In this instance, it is preferable for a child to have the GPS function on their devices turned on at all times.

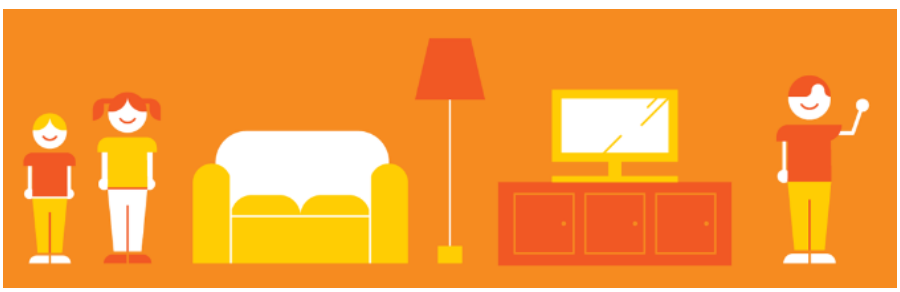
Please note that at the time of this manual being written, The Department of Health and Human Services Child Protection, Victoria, Australia, do not have set guidelines to advise on tracking children's movements, should they abscond. In the case of a child's safety/if the child in your care absconds, please consult with your agency worker and management. Safety of the child is always paramount, however so is their right to privacy. Carers need to liaise closely with their workers and not make the safety assessment of the child alone.

Agencies will need to factor in when tracking a child in care who absconds:

- Agency workers should have a set social media account to track the child in care. Workers should not use their own personal social media pages.
- Agency workers should not befriend a child on social media, but if management agree to use a a set account to make contact with a child, the worker needs to make it clear who they are when making contact. It is not appropriate to trick the child into thinking they are speaking to another child.

Please refer to the earlier pages in this manual, regarding ongoing discussions with a child regarding sharing their passwords with carers, and having ongoing discussions with regards to general cyber safety, but also their physical safety should they meet someone they met online.

With regards to children who chronically abscond, carers may find applications such as Find My Phone convenient; however carers need to be wary about installing these applications onto a child's phone in a secretive manner. Secretly installing a tracking app on a child's phone will break down the trust between a child and carer, if the child discovers the app. If carers are concerned with a child's safety, it would be preferable instead to speak to the whole household about agreeing to register their phones with these apps and leave the GPS function on at all times, should their phones be "stolen".



Kids GPS Watches

The availability of children's GPS watches is increasing in Australia. Until recently, most GPS watches were being sold from America, which limited availability to Australian carers.

An example of Australian GPS watches for children can be found at https://moochies.com/FAQ

GPS watches are aimed at primary-school aged children. They advertise perks such as:

- Tracking a child's whereabouts at all times.
- The ability for a child to call carers directly.
- Games for the child to play on the watch.

Although tracking a child has appeal to carers, please consider the following if you would like to purchase one:

- Is it being used as a deceptive ploy to track an absconding child? Carers should sit down with and explain to children about what it is, and why they are going to use one.
  The child should be told that it is a safety item, should they get lost or need assistance. If it is used deceptively, issues can arise if a child realises later that it is a tracking device and will throw it away.
- Does the watch suit a child's needs? (eg. Is it for a child with an Intellectual Disability at risk of absconding/wandering?). Is the watch to give you peace of mind or for the child's safety?
- Is the child at high risk of being abducted by birth family members? Would it suit the purpose of locating them afterwards?
- If the child changes foster homes, who controls the watch's account? (is it going to be a breach of the child's privacy if the previous carer still has access to the master account once the child moves?).
- Who pays for the watch, along with the account and simcard deal?
- Consider who purchased the device. For example, if the child was given a GPS-capable watch by a birth parent, and the parent is not allowed to know where the child lives, please consider if that parent will then be able to access the child's GPS location.

Carers should consult with their worker before purchasing a GPS watch. Most children would not need one, but all cases and situations are different. Workers will also be able to guide carers on any issues from the above dot points.

Also please note that some GPS watches only operate on 2G or 3G networks, which are not as easily accessible in some areas. At the time of writing this manual, 4G and 5G networks are becoming primary networks, and 3G networks may be turned off in some areas in the near future.

Mobile Phones for Children

Giving the child a mobile phone appropriate for their age

When giving a child a mobile phone, think about what type of phone/deal is appropriate for their developmental level.

Smart Phones:
eg. iPhone & Android-based phones

When considering phones:

- Is the phone purely for emergency calls/messages to carers? (eg. If the child is catching a bus home, or able to go out to visit friends) If this is the case, buy a handset that is not a smart phone (aka a 'dumb phone'). Dumb phones also have perks such as FM radio and MP3 (music player) capabillity.
- Is the child at a developmental level whereby they can be responsible with having access to the internet when carers are not around? A smart phone will suit, but be aware that a child with a smart phone will be able to access wifi networks, even if they run out of data on their plan. Be aware that you will not be able to track a child's internet activity with a smart phone.

When considering phone deals:

'Dumb Phone'
(Phone that is not a 'smart phone')

- Do not place a child on a monthly plan. Be aware that most phone companies who give out phones on a plan will charge a lot of money if the children go over their internet data usage limit.
- All children should start off with a pre-paid deal. This means they cannot spend more on calls/messages than the deal allows. If the plan has a set data-limit, the sim card's ability to use the internet will disconnect if they go over that limit.
- Make the decision if you want to tell the provider to barr the simcard from using mobile data (internet the sim card provides). Depending on the phone given, a child may still be able to use wifi at home or shopping centres, but at least this can limit their online activities. The adolescent's maturity should also be taken into account when making decisions regarding this

.

Most children will want the newest, best phone on the market. It is okay to say No, and have them earn that privilege as they show maturity with appropriate phone/internet use. As a general rule, a child in primary school does not need a mobile phone unless there are special circumstances.

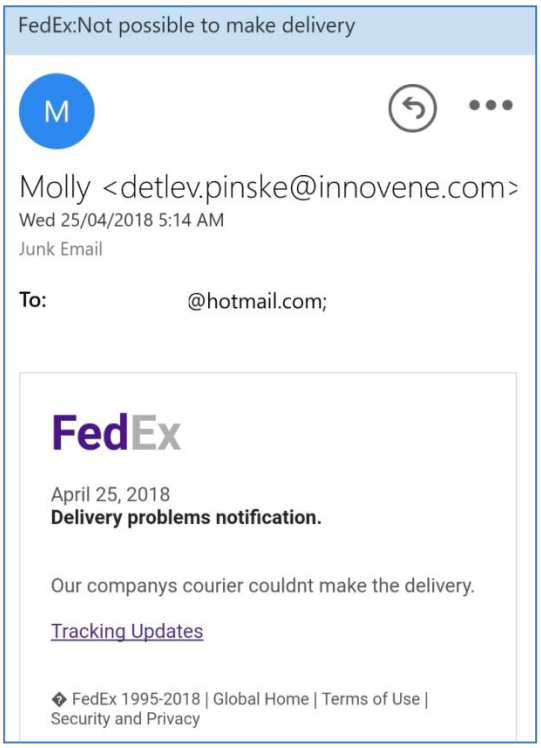
Scams

Be aware of online scams. Some emails that you receive can seem real and can trick you into giving out your passwords and other identifying information. Some emails may say “your account is being deactivated unless you click the link provided and log in”, while some try to make you click their attachment to read an ‘unpaid bill’, which is really a virus trying to take over your computer.

Please check the email address of the sender and the web address at the top of each webpage. For example if you receive an email from Ebay, and it asks you to reset your password, is the email sent to you from ebay@abcdef.info.com? If you’re not sure, close the email, and take yourself to the Ebay app/website to see if the email also appears in the legitimate Ebay inbox.

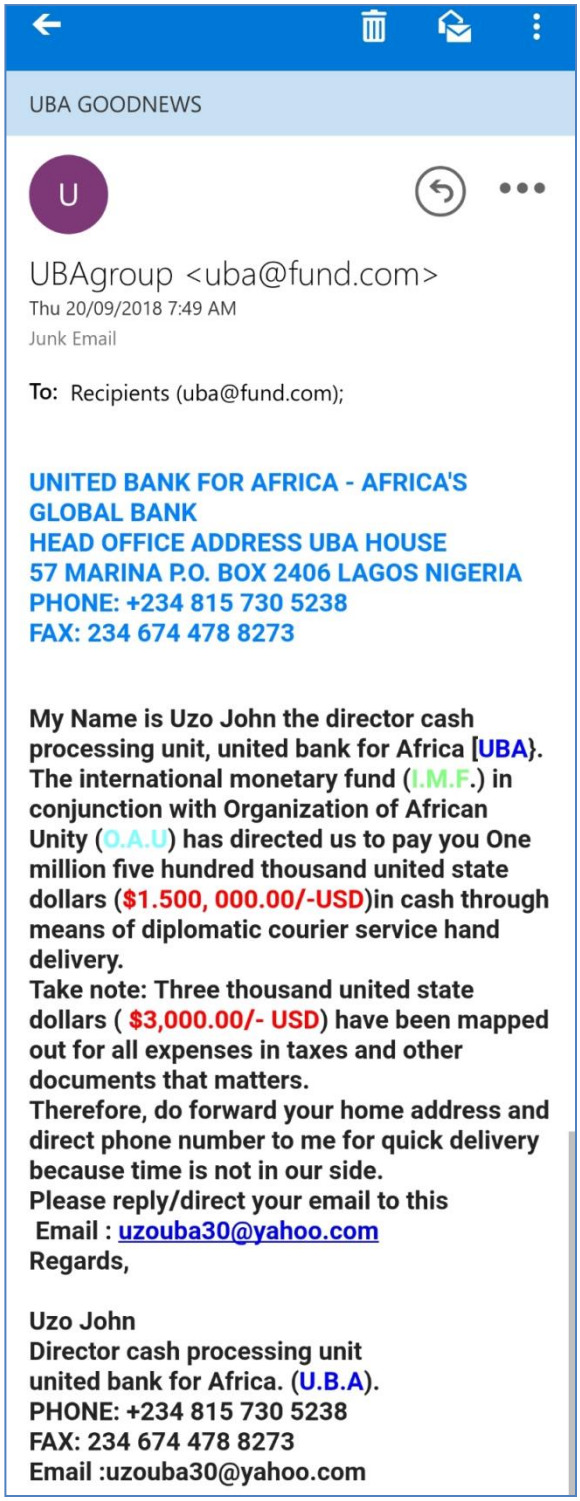
Be cautious of organisations that ask you to access your account online by inputting your full-name, address, phone, credit card details and date of birth. These are often scams to obtain your details. This is also called Phishing (pronounced ‘fishing’).
When doing research on the types of scams being used, include children in your home, to initiate conversations about the dangers of these scams.

Further information can be found at
https://www.scamwatch.gov.au/



Families can make it a fun game to see if they can spot a scam email as it comes in. This can start conversations about how to learn to read what is a fake email or not.

Here are two examples of scam emails (left & right)

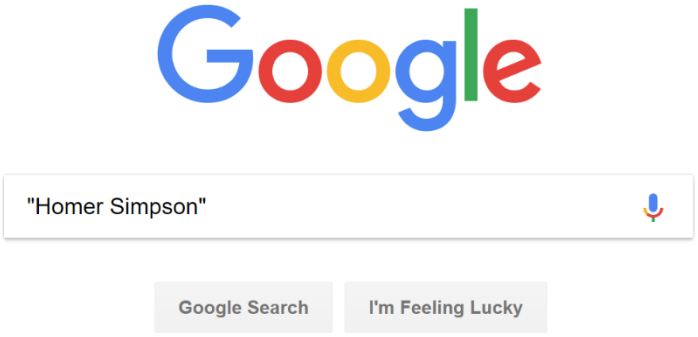


How to Google Yourself

It is good practice to Google yourself every 6-12 months, to see what others can see if they try search cares and children.

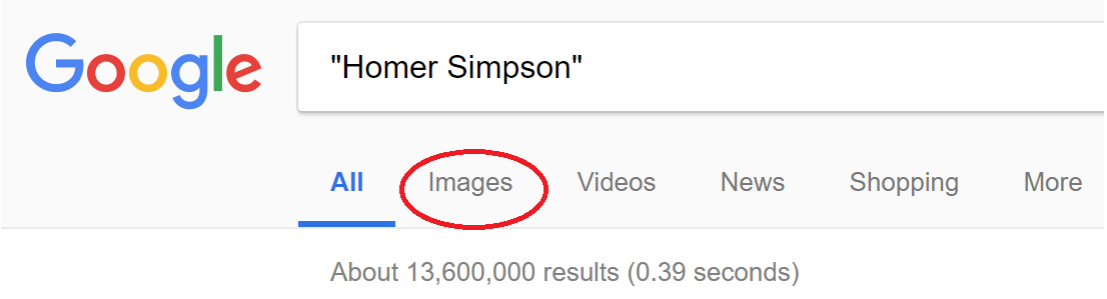
Try Googling a few different ways:

- Name on it's own. Eg. *Homer Simpson*
- Name with the talking marks *"Homer Simpson"*
- Name with an identifying piece of information that someone may use *"Homer Simpson" Melbourne*
- Search for commonly used usernames or internet nicknames used.



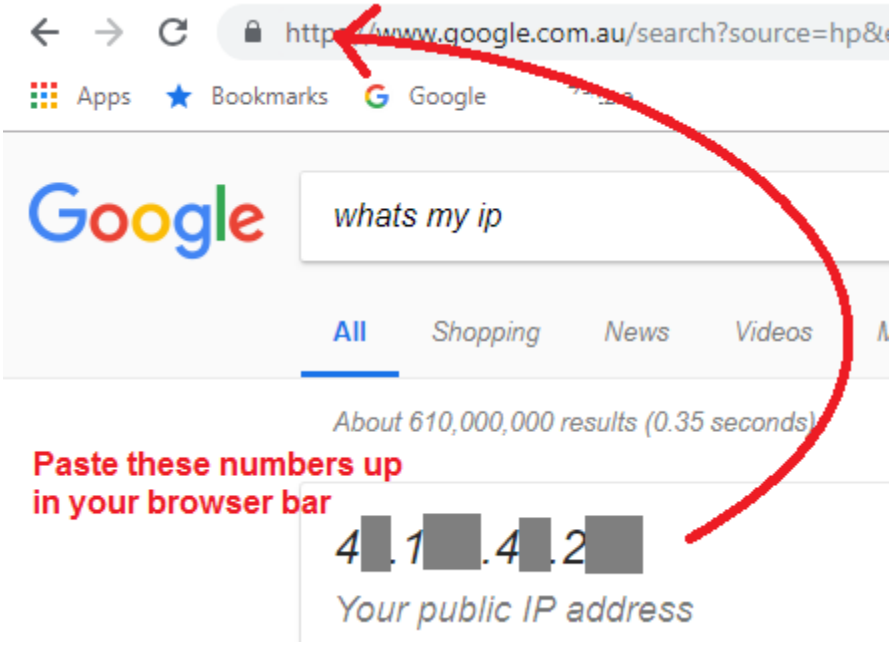
Google will often show thousands of search results. Take time to search through at least the first 10 pages of results to see if anything identifiable comes up.

Don't forget to look at the images available too.



How To Change Your Home Internet/Wifi Password:

- Google “what is my IP?”
- Copy and paste the number provided (your IP) into your browser (where you type web addresses into)



- Log into your internet settings with your account username and password (sometimes the username is *Admin* and the password is *password*).
- Change your Wifi password
- Save (and don’t forget what your new password is!)

Additional Government Resources

On the following pages, here is a list of resources released by the Victorian Government.

Department of Health and Human Services Child Protection: Information Sheet for Foster Carers

This handout was distributed in Melbourne in July 2012. The main point to take note of in this handout is that photos of children cannot be posted online if it labels the child as a child under a court order. This includes using captions labelling the child such as “foster child”, “child in our care”. Instead, use captions such as “our family trip”.

Posting information that leads to identifying a child as being subjected to a Children’s Court order is considered ‘unlawful’ and can lead to carers being fined or imprisoned.

Carers are advised to consult with their worker or support agency regarding this matter if they are unsure of their rights and responsibilities regarding social media.

This can also be viewed via the Foster Care Association of Victoria’s website here:
https://www.fcav.org.au/images/carer-resources/articles-publications/DHS_Social_media_and_foster_careOct13.pdf

Additionally, carers can obtain further information about *Photos On Social Media* from the Foster Care Association of Victoria Website here
https://www.fcav.org.au/images/carer-resources/information-sheets/Photos_and_Social_Media.pdf

human services

INFORMATION SHEET FOR FOSTER CARERS

1. The posting of photographs and social media

This information is designed to provide foster carers with practical information and advice on the use of social media and the posting of photographs of children in foster care, and what action needs to be taken by carers to protect children's rights and ensure their wellbeing.

Photographs are important mementos that record children's history, achievements and life experiences. However it is important that foster carers are aware of the risks of posting photos using social media. When photos are posted on-line and shared through social media they can be downloaded, manipulated, reused and retransmitted freely by others, without any control by the photo's owner.

It is also important that foster carers understand the legal implications of using social media and know how to avoid breaching the law. The right to privacy must also be considered; a child or their family may not want their situation revealed on social media.

It is important to have a discussion with your agency worker if you require further information, advice or support before deciding whether or not to post photos of children in care, on social media.

2. Social media defined

Social media is the term used for internet-based tools for sharing and discussing information among people. It refers to user-generated information, opinions and other content shared over open digital networks.

Social media may also include (although is not limited to):

- social networking sites (for example Facebook, Myspace, LinkedIn, Bebo, Yammer)
- micro-blogging (for example Twitter)
- video and photo sharing websites (for example Flickr or YouTube)
- forums, discussion boards and groups (for example Google groups, Whirlpool)
- instant messaging (including SMS)

3. The law

Children, Youth and Families Act 2005

The *Children, Youth and Families Act* 2005 is the legislation that provides for the protection of all Victorian children.

It is not unlawful for a photo of a child who is in out-of-home care to be posted on social media.

It is unlawful to publish information that is likely to lead to the identification of a child as being subject to a Children's Court order, regardless of whether or not this information accompanies a photo. Such information includes (but is not limited to):

- the name and address of a child
- identification of their school
- the relationship of a child to identified relatives or their association with friends, officials and professional acquaintances.

Restrictions on the publication of information likely to identify a child as being subject to court proceedings is broader than social media (includes print media) and applies to all persons in all situations; except with the permission of the President of the Children's Court, or of the Secretary of the Department of Human Services. A breach of the Act can result in prosecution and lead to a fine of up to $12,214 or two years imprisonment.

Information provided to foster carers about a child by the department or foster care agency as part of the placement matching process, or via a confidential report cannot be used by a carer beyond informing their decision to accept a placement or to provide appropriate care for the child. For example, a carer can disclose a medical condition to a registered medical practitioner for the purpose of providing medical treatment or services to a child but cannot disclose a child's medical condition to friends, family or anyone else, where the disclosure serves no medical or care related purpose. A breach of the Act in this regard can result in prosecution and lead to a fine of up to $1,221.

The *Charter of Human Rights and Responsibilities Act 2006*, the *Information Privacy Act 2000* and the *Health Records Act 2001* also contain provisions to protect and promote human rights, privacy and fair and responsible handling of information between government, agencies and individuals.

4. Avoiding a breach of the law

Foster carers are not responsible for monitoring or enforcing controls on the use of social media by others outside their immediate care and control i.e. adult members of the community, other people's children.

Foster carers are encouraged to notify their foster care agency if they have concerns about the impact of the use of social media on children in their care. Carers need to instil safe and responsible social media practices with children for whom they care.

A common sense approach is to never identify a child as a foster child, or a child in care, a child subject to a court order (past or present), a child subject to court proceedings or child protection involvement (past or present) or identify a foster carer when pictured with a child in care.

5. Other considerations

Consider the child first. Children in care, their parents and family have a right to privacy and their wishes need to be considered and respected. A child or their family may not want other people knowing that they are in care. Commentary which accompanies photos on social media with identifying references to the child's care situation, the 'foster carer' or 'foster care' household must be avoided.

Consult as appropriate. The Charter for Children in Out-of-Home Care includes the right for a child to be treated with respect, to have a say, and be heard. Posting photographs with accompanying non-sensitive information on social media such as the child's sporting accomplishments may seem innocent, but even if it does not breach any of the laws defined above, it may be contrary to the child's wishes. Speak with the child first and if appropriate, use their care team to seek the views of the child's parents, extended family, caseworkers and other professionals.

Be aware. Check the terms and conditions of social media platforms. Set privacy settings. Protect your personal information and consider anything posted on a social networking site as public. Use this information sheet and seek advice from your foster care agency when you are unsure about compromising the privacy of children in care or their families.

6. Further information

For further information, support and advice contact your foster care agency (Community Service Organisation).

Senior officers within the Department of Human services can provide Community Service Organisations advice on individual and complex matters. Further information on the law, Charter for Children in Out-of-Home Care and cybersafety is available at www.legislation.vic.gov.au, www.dhs.vic.gov.au and http://www.cybersmart.gov.au/.

Glossary of Computer and Internet Terms

Apps (aka Applications)
Apps are the name of programs designed for use on smart phones or mobile devices such as tablets. These can be anything from social media apps, health-tracking apps, etc.

Archiving
When websites move old content to a database. This helps keep new content at the front of webpages, apps, etc. . Archiving can change the web address of an article, or location of photos/content on a website.

Cookies
Cookies are a feature on the computer that remember your web addresses, some passwords, and some personal information when you are browsing the internet. They are usually already turned on on all computers unless you specifically turn them off.

Downloading
Saving or copying information or photos from the internet to your home computer.

Homepage
The webpage that first appears when you open your internet application (such as Internet explorer). Users can set which webpage they want to appear on the home page.

Hardware
The electronic parts inside the computer/device.

IP (Internet Protocol)
The IP is unique for all internet accounts (it looks like a series of numbers with full stops between them). Each device that connects to the internet has an address that can be tracked. This is what the police can track if illegal activity occurs online.

ISP (Internet Service Provider)
The internet package provided to you by a provider such as Telstra, Optus, Dodo, etc. The ISP provide you with a unique IP address.

Modem
The modem is the device that receives the digital 'Internet' signal through the phone line. It tends to look like a box or a portable USB stick (also known as a 'dongle'). The modem can either plug directly into a computer, or send a Wifi internet signal to the household computer, laptop or tablet that can pick up a wireless signal.

Operating System
The operating system on a computer or smartphone is the program used that controls the computer or phone. Computer operating systems can include Microsoft Windows 7 or 10, (Apple) Mac OS and Linux. Smartphone (or Mobile OS) examples are (Google) Android and (Apple) iOS.

Screenshot
This is a photo taken of what is on the screen. This can be on computer or on a smart phone. This is handy to do when needing to copy conversations when being bullied, keeping copies of receipts, or ideas for future reference.

Servers
There are different types of servers, which serve different purposes; from storing files on the internet, providing website hosting, listing and storing data and files for companies, etc. These servers are programs, however there are also physical servers/hardware. The internet operates off severs (which look like rooms full of computer hard drives) based all around the world. Every piece of data posted online gets saved into servers, possibly even backed up onto other servers, which is why it is impossible for information to be deleted completely.

Smart phone
A smart phone is the new generation of mobile phones that allow the user to use it like a hand-held computer. Smart phones tend to allow the user to browse the internet, send text and picture messages (MMS), read emails, play music, play movies, take photos, make calls, make video calls, play games, etc.

Software
The programs on your electronic device (computer/tablet/phone).

SPAM
Spam is mostly just advertising emails, which users would not normally receive (such as get rich quick schemes, identity-theft emails, and selling non-tested medications). This is why Spam is referred to as 'Junk Mail'. Spam is typically sent to random email addresses by people the users do not know. These emails need to be blocked and deleted.

Trolls
Trolls follow public online conversations and create conflict with hurtful messages and malicious instructions instead of helping. Victims tend to react with outrage. Continued abuse is called 'Trolling'. Trolls need to be ignored, blocked, and reported to the website's administration.

Uploading
Sending information or photos from your device/computer to the website and/or the Internet. Every piece of data uploaded gets saved into servers belonging to that website, which is why it is impossible for information to be deleted completely.

Webcam
A Webcam is a camera that is mounted on or in the computer/laptop, sending a video signal or photos from the computer directly to the internet. For example, it can be used for video diaries (such as those found on YouTube) and video calls (such as Skype).

Wifi
Wifi is internet that is broadcasted by a modem/router with an antenna. Laptops, iPods, and mobile phones that have Wifi capability (can pick up the Wifi signal) can connect to the internet by picking up the signal.

Glossary of Facebook and Social Media Terms

Here are some Facebook-specific terms along with some general social media terms.

Avatar
A digital representation of someone online. This 'person' created on apps and games can look like the person creating it, or can look completely different. Profile pictures are also avatars.

Bio
'Bio' is short for biography. This is usually a short description of the person holding the account. Bio's tend to list what a person's interests are, or personality traits.

Block list
The list of Facebook users that you have selected to stop seeing your Facebook page. If you block someone, they cannot see your activity and vice versa.

Check in
Checking into a location (or venue, country, or event) lets the friends of Facebook users know where they are. Some people like to check into a venue to boast about their whereabouts, however carers of children in foster care need to be aware that this is not ideal if there are any safety concerns from the child's birth family. Carers and children using this feature need to be aware of who their friends are on Facebook, who will be seeing where they are. Also factoring in if the post is made public to people outside their friends list.

Clickbait
When there is an ad, video or photo with a description that is misleading or sensationalised. The idea is that it causes readers to click the link. Often these are labelled along the lines of "you wont believe..", when the content itself is a virus, scam or has content not what was advertised. Some websites do it to increase the amount of traffic to their websites.

Cover Photo
This is the long horizontal image on top of a person's Facebook profile page. Businesses can use it to put their logos or advertise some of their content.

Emoji
An Emoji is a small image used to express an idea, emotion, etc. Typically used in text messages and typed conversations on social media.

Event
A Facebook feature that lets the general public or organizations promote events such as parties, food truck festivals, shows, etc. It is a good promotional tool for organisations, but families need to be very careful when advertising events such as birthday parties. If the event is not listed as *private*, it could be viewable to the whole world. This has caused issues whereby uninvited guests attend. In extreme cases, house parties could have gatecrashers, resulting in violence and consequently police attendance.

Facebook Chat (also known as Private Messaging or Direct Message)
The chat feature lets Facebook users send messages, photos and videos to people privately. This can be done via the Facebook Messenger application on mobile phones, or via the Private Message button on the computer. The Facebook Chat application works like text messaging or emailing, sending messages from one account to another, without the rest of the Facebook community seeing the messages. Even if carers befriend their foster children on Facebook, any messages the child sends through this system cannot be seen by the carer.

Facebook Friend
A friend on Facebook is someone who you have "added". This adds them to your "friends list". They can then access information and statuses you've posted on your Facebook account.

Facebook Live
A feature that lets users load a video (also known as streaming a video) onto Facebook in real time, as it happens, as they are recording it.

Facebook User
A person using Facebook.

Follow/Following
This is the name given to a feature that allows you to choose to subscribe to seeing posts from other people/pages/groups on your newsfeed.

Friends List
This is the list that is created when you befriend people on Facebook. Anyone else on this list can see who else you are friends with on Facebook.

Games and applications
Facebook has many games that can be played online. When installing these apps, at times, a pop-up will appear and warn you that sometimes your information will be shared by third-parties, or your information or scores will appear on other people's Facebook news feeds. Many apps now require you to log into Facebook. This also allows games to prompt you to advertise the game for free, by sharing your points with others and invite them to play too.

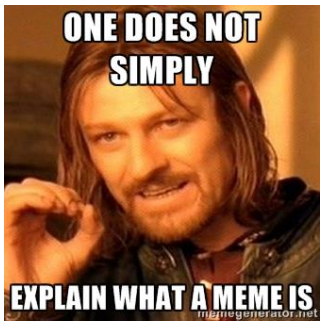
GIF
It's a type of image file, with a short series of images pieced together to look like a short (often 3 second) video.

Groups
Groups are as the name suggests. It is a Facebook page that allows people with similar interests gather online. They usually share a wall, which acts as a notice board for all users to add to. Some groups are locked. This means that only those who are invited to join the group can see what is written on it. If a user adds content to a locked page, it will not appear on their friends' Facebook feeds.

Hashtag
A Hashtag is used to make a key search word for users. Putting a # in front of keywords when writing captions for photos and at the end of status updates, allows for the post to be found by anyone else searching that hashtag. For example, listing *#Funny* in a post means that anyone who searching that hashtag or topic, can potentially see any posts across the globe with that hashtag.

Like
Clicking the Like button on a picture allows a user to show they are interested in the content posted by others. Likes now also include options such as a thumbs up, a sad face, an angry face, etc. Liking a post can show on your friends Facebook feeds. Many youth feel the need to post pictures to get more and more Likes, as a misconception that this means more people care about you.

Meme
It is a way of turning a picture or saying into something comical. Often the meme is related pop culture references, making fun of a picture, or about a saying, movie or song, Pronounced “meem”.



Mention
It is a way of tagging someone’s name into a comment or status. The person mentioned gets a notification of it too. It is a way for users to say who they are with, who they’re talking about or responding to a conversation.

News feed (also known as “Feed” or “Facebook Feed”)
The ‘News’ that Facebook automatically sends out to show your activity on Facebook (what pictures/ posts you’ve liked, who’s pictures you added comments to, what messages you have written on other people’s walls, etc) It also shows what the people on your friends list have been doing.

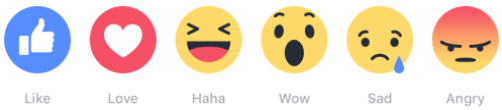
Notifications
Notifications are alerts that Facebook sends users. They advise you if someone ‘Liked’ one of your pictures, or commented on of your status updates. Users can also tailor their Facebook account to notify them when others have commented in groups they’re members of, pages they’ve liked, etc.

Profile page
The Facebook page that Facebook allocates to each member of Facebook. As the name suggests, it is a page where users can list their details and build a profile. Profile pages can be locked, so that only one’s Facebook friends can see the bulk of the photos/videos/statuses posted there.

Profile Picture
This picture is located on the top of your Facebook profile page. All profiles have a “profile picture”. This can be seen by *everyone*, regardless if they are you are a Facebook “friend” or not. If you are concerned about this, then profile pictures do not need to be a picture of the actual person, but rather a picture that represents the user.

Privacy Settings
Privacy settings allow users to choose how they would like Facebook to distribute their information, photos and statuses. The best option is to adjust the account settings so that only Facebook Friends can view all posts. Do not allow your Facebook page to be viewable to *Everyone* (this means anyone across the globe can see your page, indicated by a small picture of the globe at the top of your posts).

Reactions
Facebook now has Facebook Reactions, that allow a user to express how they feel about a post. At the time of writing this manual, the options Facebook offers are to Like, Love, Haha, Wow, Sad or Angry.



Selfie
Taking a photo of yourself. Usually done on a mobile phone, where you can see your image on the screen as you take it.

Share
It is a way of someone re-posting content they’ve seen, placing it onto their own social media page for other’s to also see.

Status Updates
Let users write a short something about what they are doing (which can include writing sentences or uploading a picture/video with a caption). One thing to take note of is that Facebook can sometimes list the suburb that users were in when you updated the status, particularly if they’ve updated it via mobile, and have their GPS location turned on. Status updates appear on the news feed of people on your friends list.
Users need to be aware that privacy settings can be adjusted so that posts can be seen by *Everyone* (the whole world whether they’re Facebook friends or not), or *Friends only* (so people who are not Facebook friends cannot see the posts). It is ideal to adjust the privacy settings to *Friends only* for all posts.

Stories
On Facebook and Instagram, Stories are a way of users being able to post pictures or videos, which will only be available on their profile for moments, a day, or a week. This is a way of posting content without it remaining on a profile page forever.

Tagging

When a person uploads photos onto Facebook, Facebook lets them ‘tag’ who’s in the photo. It essentially links a person’s Facebook account to any photos that they are tagged in. The tagged person’s friends can then see these photos, even if their photo’s from an album belonging to someone who is not their friend.

When uploading photos onto Facebook, a prompt can sometimes appear asking the user to allow Facebook to automatically tag friends, using facial recognition software. It is preferred that users do not use this function, as this function in the past has changed the user’s computer code and opened the user and their friends to threats from hackers.

Users can also “untag” themselves from photos other people post and tag them in. This removes the link of the photo to the user’s account, but it doesn’t remove the photo itself from the other person’s Facebook page.

Facebook also allows users to “tag” their friends in written statuses, which means that the status will link itself to not only the writer’s page, but also to the page of the user who was tagged.

By adjusting privacy settings, users can approve, hide or block statuses and pictures that they’re tagged in.

Trend

A trend is as the name suggests, topics that are popular in the moment on social media. This is usually tracked by a hashtag or key word.

Unfollow/Unfriending

This is the name given when removing someone from your friends list.

Wall

Every Facebook profile page has a wall. The wall works like a personal message board. Users can write on a person's wall if they are friends with them. There is a box at the top of each wall. This box allows users to update their statuses and share photos, videos, links and other application content. Things shared will appear as posts on the user’s own profile, tracking each user’s activity.

Glossary of Chat Slang

Children and adults often use slang words and abbreviations when chatting online.
Below is a list of some commonly used ones.

Many of these can be found at: http://www.netlingo.com/top50/acronyms-for-parents.php
and https://securingtomorrow.mcafee.com/consumer/family-safety/2018-texting-slang-update-decode-teen-saying-online/
also, https://www.bark.us/blog/decoding-teen-text-slang/

121- Let's chat in a private message
182- I hate you
2nite – Tonight
2mz or 2moro or Tom- Tomorrow
8 - Oral sex
9, CD9 or Code 9- Parents are nearby
99- parents are gone
1337 - Elite
143 - I love you
182 - I hate you
1174 - Nude club
420 - Marijuana
459 - I love you
A3- Anytime, Anywhere, Anyplace
ADR or Addy - Address
AEAP - As Early As Possible
ALAP - As Late As Possible
ASL - Age/Sex/Location
ATW- All The Way
AWGTHTGTTA - Are We Going To Have To Go Through This Again
Banana - code word for penis
BD – Big Deal
BESTIE- best friend
BION- Believe It Or Not
B4YKI - Before You Know It
BRB - Be Right Back
CD9 - Code 9 - it means parents are around
C-P - Sleepy
CYT - See You Tomorrow
CYA- see ya
DIKU- Do I Know You?
DND- Do Not Disturb
DWB- Do not Write Back
DOC - Drug Of Choice
DW- Don't worry
DWB- Do not Write Back
E- Ecstacy (drug)
E123 - Easy as One, Two, Three
EM - Excuse Me
EOD - End Of Day -or- End Of Discussion
F2F - Face-to-Face
FOMO - Fear of Missing Out
GGP- Gotta Go Pee
GNOC - Get Naked On Cam
GOMB- Get off my back
GYPO - Get Your Pants Off
HAK - Hugs And Kisses
Hazel- Heroin (drug)
HT- Hi There
IDEK- I don't even know
IKR- I know, right?
ILU - I Love You
I&I - Intercourse & Inebriation
IDGI - I Do not Get It -or- I Do not Get Involved
IDKWTD- I don't know what to do
IMEZRU - I Am Easy, Are You?
IMHO - In My Humble Opinion
IRL- In real life
J/O - Jerking Off
JK – Just kidding
KITTY - code word for vagina
KOTL - Kiss On The Lips
KFY -or- K4Y - Kiss For You
KPC - Keeping Parents Clueless
KYS / KMS- Kill yourself / Kill myself
L8R - Later
LMIRL - Let's Meet In Real Life
LMAO - Laughing My Ass Off
LMFAO- Laughing my F***ing Ass Off.
LOL - Laughing Out Loud
LTM- Laugh To Myself
LY- Love Ya
LYAAF- Love you as a friend
MOOS - Member Of The Opposite Sex
MOSS - Member(s) Of The Same Sex
MorF or **RUMORF** - Male or Female
MOS - Mom Over Shoulder
MPFB - My Personal F*** Buddy
MUSM- Miss You So Much
NALOPKT - Not A Lot Of People Know That
NIFOC - Nude In Front Of The Computer
NFG- No F***ing Good
NMU - Not Much, You?
NM - Never Mind -or- Nothing Much -or- Nice Move
NP - No Problem -or- Nosy Parents
NUB or NUUB- New person to a site or game

OMW - On My Way
OTP - On The Phone
OIC - Oh, I See
OMG - Oh My God
OMFG - Oh My F***ing God
OT - Off Topic
P911 - Parent Alert
PAL - Parents Are Listening
PAW - Parents Are Watching
PHARMING- Getting into medicine cabinets to find drugs to get high on
PIR - Parent In Room
PM- Private Message
POS - Parent Over Shoulder - or- Piece Of Sh**
POV- 'Poverty' explaining someone/something being poor
Pron - porn
QT - Cutie
RU/18 - Are You Over 18?
RUH - Are You Horny?
ROFLMAO- Rolling On the Floor Laughing My A** Off
SO - Significant Other
STBY - Sucks To Be You
SH - Sh** Happens
SU- Shut Up
SUSS- Suspicious
SWAK- Sealed With A Kiss
THX or TX or THKS - Thanks
TCOY- Take Care Of Yourself
TDTM - Talk Dirty To Me
TMI- Too Much Information
TTFN - Ta Ta For Now
TTYL - Talk To You Later
UAPITA- You are A Pain In The Ass
Ur - you are
WHITE LADY- Cocaine/Heroin (Drugs)
WFM- Works For Me
WTF - What The F***
WUF - Where You From
WYCM - Will You Call Me?
WYRN - What's Your Real Name?
WYWH - Wish You Were Here
XOXO - Hugs and Kisses
YOLO- You Only Live Once
YW- You are welcome.
Zerg - To gang up on someone

Emoji slang

An Emoji is a small image used to express an idea, emotion, etc. Some are used as code or slang.

🍆 🍌 The eggplant or banana emoji is used to refer to the penis.

🍑 The peach emoji is used in sexting, referencing the butt or women's genitalia. Cherries as breasts 🍒

💦 The "sweat" emoji is mostly used to mean "ejaculate," often used in conjunction with the tongue emoji 👅💦

The following emojis can also describe sex: 🌮 (taco), 🚇 (train in tunnel),

More examples can be found here; https://educateempowerkids.org/common-emojis-used-in-sexting/

About the Author

(Above picture) Virginia Papadopoulos promoting the OzChild Cyber Safety Manual at the IFCO *International Foster Care conference. In Sydney, 2015.*

Virginia Papadopoulos has worked in the OzChild Foster Care program for 9 years, seeing first-hand the cyber safety issues that can arise for children in care. Virginia has created this Cyber Safety Manual, which is one of the first manuals to be released in Melbourne, Australia, that is specifically aimed towards carers.

The reason the manual was created was to help carers understand the significant risks posed by social media.

"*The manual's main message is to not ban the internet from children, but to be aware of the dangers and educate children. That way the whole family can remain cyber safe, through continued communication and education.*"

The manual was created in 2012, in response to feedback from foster carers that they needed more education on cyber safety issues that relate specifically to children in care.

Since its creation, the Cyber Safety Manual has been shared with thousands of people online.

In October 2012, the manual was presented at the FCAV (Foster Care Association of Victoria) Melbourne Foster Care Conference. Over 100 physical copies were distributed to agency workers and carers.

In February 2015, the OzChild Cyber Safety Manual was picked up by Melbourne Foster Care agency Salvation Army WestCare, who posted it to Twitter where it was seen by over 2000 people.

In November 2015, the manual was advertised at the IFCO International Foster Care conference in Sydney (pictured right), bringing support to families and agencies worldwide.

In 2016, the manual was picked up by international Foster Care agency Key Assets for their training of their staff and carers in Australia and Scotland.

In September 2017, the manual was presented at the Melbourne Shine a Light foster care conference.

In 2018, the manual has been showcased at Cyber Safety Trainings through Carer Kafe (run by the Foster Care Association of Victoria/Department of Health and Human Services).

About OzChild

For over 160 years, OzChild has been committed to the protection of Australia's most vulnerable and at-risk children. In service to this commitment, OzChild is also an advocate for sector reform and positive public attitudes to children in care. We conduct high-quality, independent research into every aspect of child welfare within Australia and around the world

OzChild works with over 6,000 children and young people with the aim of providing them a better future. OzChild often works with children who are in the 'too hard' basket in the belief that every young person deserves the chance to shine. Our approach is comprehensive; where we can provide multiple services to address the often numerous issues in the lives of children and their families.

Our programs range from

- Foster care for children aged 0 – 18 who can no longer live with their parents
- Services for children with disabilities
- Health and welfare support such as counselling in schools and for families experiencing difficulties
- Respite for families whose children often have complex needs
- Education, scholarships, mentorship and development programs for disengaged and underprivileged youth.

OzChild has recently engaged in the implementation of Evidence-Based Services in Victoria, New South Wales and Queensland, such as SafeCare, Functional Family Therapy- Child Welfare (FFT-CW) and Treatment Foster Care Oregon (TFCO).

For more information, please visit the OzChild website at
http://www.ozchild.org.au/

Bibliography

Here is a list of the resources referred to in this manual.

ACORN: Australian Cybercrime Online Reporting Network https://www.acorn.gov.au/

ACORN Online Child Abuse Material
https://www.acorn.gov.au/learn-about-cybercrime/online-child-sexual-abuse-material

Club Penguin - A social website aimed at children 6-14 years of age.
https://www.clubpenguinisland.com/

Common Sense Media https://www.commonsensemedia.org/

Cyber Bullying article, The nature of cyberbullying, and strategies for prevention, Slonje et al 2012, obtained from http://agnesday.com/wp-content/uploads/2012/10/Slonje-Cyberbullying.pdf

Department of Human Services Social Media Information Sheet for Foster Carers. Obtained through the Foster Care Association of Victoria website: http://www.fcav.org.au/images/carer-resources/articles-publications/DHS_Social_media_and_foster_careOct13.pdf

Deviant Art - A website dedicated to art, with users able to create an account and post their artistic talents online. www.deviantart.com

eSafety Commissioner Homepage: (previously named Cyber Smart). https://esafety.gov.au/
Specific eSafety information for families can also be found here https://esafety.gov.au/esafety-information/esafety-issues
More information on Parental controls can be found at the eSafety Commisioner's website here
https://www.esafety.gov.au/education-resources/iparent/online-safeguards

eSafety Commissioner Sexting page https://www.esafety.gov.au/esafety-information/esafety-issues/sexting

Family Zone- A parental control program designed for families to use, promoting online safety.
https://www.familyzone.com/au/

Family Zone Article: The Five Real Costs of Online Gaming article: https://www.familyzone.com/blog/five-costs-of-online-gaming

Facebook - Facebook is the most popular of the social networking websites. www.facebook.com

Facebook Helpdesk For users requiring assistance with cyber safety settings.
https://www.facebook.com/help/?ref=pf

Fernwood Fitness: How to deal with cyber bullies factsheet- https://www.fernwoodfitness.com.au/Weight-Loss---Exercise/Well-Being/How-to-deal-with-cyber-bullies/

Flikr - A website designed for sharing photos, used particularly for those passionate about photography.
https://www.flickr.com

Fortnite: The Guardian news article: **Fortnite: a parents' guide to the most popular video game in schools**
https://www.theguardian.com/games/2018/mar/07/fortnite-battle-royale-parents-guide-video-game-multiplayer-shooter

Foster Care Association of Victoria - https://www.fcav.org.au/
Good Practice on Social Media Guidelines
https://www.fcav.org.au/images/carer-resources/information-sheets/Good_Social_Media_Practice.pdf
Photos and Social Media Guidelines
https://www.fcav.org.au/images/carer-resources/information-sheets/Photos_and_Social_Media.pdf

Fox news article: 5 dangerous apps that you don't know your kids are using
http://www.foxnews.com/tech/2015/01/31/5-dangerous-apps-dont-know-your-kids-are-using.html

Habbo- A chat program which is aimed towards use by children and teens. www.habbo.com

Instagram - A form of social networking that allows users to follow one another through photos.
https://www.instagram.com/

Kiddle- Safe Visual Search Engine for Kids. http://www.kiddle.co/

Kids Helpline Sexting factsheet. https://kidshelpline.com.au/teens/tips/sexting-and-the-consequences/

Kik Messenger - An instant messaging application for mobile phones.http://www.kik.com/
Kik's guide for parents. http://www.kik.com/uploads/files/Kik's%20Guide%20for%20Parents%20-%20February%202017.pdf

Lawstuff: know your rights
http://www.lawstuff.org.au/vic_law/topics

Media and Communications in Australian Families: Report of Media and Society Research project. December 2007. Obtained from
http://www.acma.gov.au/~/media/mediacomms/Research%20library%20reports%20old/pdf/maciaf2007_overview%20pdf.pdf

Minecraft
A game where children can create their own world by building/digging, creating lands with the use of 3D blocks.
https://minecraft.net/en-us/

Moochies (Kids GPS watches) https://moochies.com/FAQ

Moshi Monsters - An educational networking game for kids of all ages. www.moshimonsters.com

Myspace - A social networking site dedicated to those who wish to share and promote musical talents.
https://myspace.com/

Parental involvement in preventing and responding to cyber bullying CFCA Paper no.4, 2012. By Elly Robinson. Obtained from https://aifs.gov.au/publications/family-matters/issue-92/parental-involvement-preventing-and-responding-cyberbullying

Pinterest - This is a virtual pinboard where users can post photos, recipes and share ideas.
https://www.pinterest.com.au/

Poptropica - A virtual world which requires children to complete tasks and socialise with others.
http://www.poptropica.com/

Reach Out: Australia's leading online mental health organisation for young people. https://au.reachout.com/
Reach Out Cyber bullying Fact sheet - https://au.reachout.com/articles/5-strategies-for-dealing-with-cyberbullying

Roblox website https://www.roblox.com/
Roblox article: *Cyber expert warns parents about gaming apps after reports of Roblox sex chat.* http://www.abc.net.au/news/2017-02-22/cyber-expert-warning-gaming-app-roblox-children/8292712

Royal children's hospital publication; Australian Child Health Poll. *Screen Time and kids: What's happening in our homes?* https://www.childhealthpoll.org.au/wp-content/uploads/2017/06/ACHP-Poll7_Detailed-Report-June21.pdf

SECASA (South Eastern Centre Against Sexual Assault)
Protecting Children from Sexual Abuse: (handout for parents)
http://www.secasa.com.au/assets/Documents/protecting-children-from-sexual-abuse.pdf
South Eastern Centre Against Sexual Assault: Respect me, Don't Sext me; Sexting Education Sheets:
http://www.secasa.com.au/pages/respect-me-dont-sext-me/
Resources for families http://esafety.secasa.com.au/grown-ups/resources/

Send this instead: an app that gives children/teens an alternative to Sexting:
https://sendthisinstead.tumblr.com/

Spotafriend website: https://www.spotafriend.co/

Spotafriend article: *Spotafriend app sees young children posting provocative selfies online*, by Jordy Atkinshon. Published in the Bayside Leader on 27/6/2017. Located via The Herald Sun website:
http://www.heraldsun.com.au/leader/inner-south/spotafriend-app-sees-young-children-posting-provocative-selfies-online/news-story/75f8746ab3dde6d51d2e73c85daf834c
Skype - Skype allows users to make video and audio-only calls to others. http://www.skype.com/en/

Snap Chat 101: What it is and How to Use it: Verizon Wireless Article, can be obtained here:
https://www.verizonwireless.com/articles/snapchat-101-what-it-is-and-how-to-use-it/

Stop Cyber Bullying – The most popular anti-cyber bullying website in the world.
http://www.stopcyberbullying.org

Scam Watch - General information about identity theft, medical scams, banking scams, competition scams, etc. http://www.scamwatch.gov.au

Staying Safe on Facebook- by Susan McLean (Australia's foremost expert in the area of cyber safety).
http://www.cybersafetysolutions.com.au/

Staying Safe on Facebook -Susan's 8-minute video with tips for carers.
http://www.generationnext.com.au/2012/08/video-interview-staying-safe-on-facebook-susan-mclean/

The Line - Helping youths understand when they are "crossing the line" in social situations.
http://www.theline.org.au/
The Line: "C'Monn… Send me a Sext..": http://www.theline.org.au/send-me-a-sext

The Social Media Glossary
https://blog.hootsuite.com/social-media-glossary-definitions/

Tumblr - This is a virtual pin board that allows users to share photos, art, text, music and videos online. www.tumblr.com/

Twitter - Twitter operates in a manner that lets users write only short sentences about what they are thinking. www.twitter.com

Undertale game https://undertale.com/

Virtual Global Taskforce (Australian branch) – The authorities protecting children from online grooming. http://www.virtualglobaltaskforce.com/
Online Child Protection form, Virtual Global Taskforce' Australian branch (Via the Australian Federal Police website) https://forms.afp.gov.au/online_forms/ocset_form

Wired Safety – An American educational tool on cyber safety, sexting, cyber bullying, cyber stalking, etc. http://www.wiredsafety.com/

Yubo- https://www.yellw.co/

Youtube - A video-sharing website on which users can upload, share, and view videos. This can include video diaries. www.youtube.com