ySafe

ySafe Cyber Safety

PARENT GUIDE

THE PARENT GUIDE TO CYBER SAFETY

Hi there!

If you've received this, we take it you came along to one of our parent cyber safety education sessions. Thanks! You've officially taken the first steps to setting up a cyber safe home for your family.

You've now also been inducted into the ySafe cyber safe community. You're joining thousands of other parents who are approaching cyber safety the ySafe way- with drive and assertiveness (we know this, otherwise you wouldn't have attended our session!) So well done! It's great to have you aboard!

In this document you'll find information that summarises the key points discussed on the night, plus some additional notes.

If you would like to get in touch with us, please feel free to contact us at anytime. You can email us at information@ysafe.com.au

Don't forget to Like us on Facebook! (@ysafesolutions).

See you soon! The ySafe Team

ySafe

KEY CYBER SAFETY RULES
FOR YOUR FAMILY

It's important that everyone in the family understands cyber cyber safety principles, and puts measures in place to ensure their safety. Some of the staple cyber safety rules that can be implemented in your home are:

- Always keep all your social media profiles on private
- Never talk to strangers and accept friend requests/follow requests from people you have never met before
- Turn off location services on all apps that don't require them to be turned on.
- Never post a photo or video of yourself in a school uniform
- Never send inappropriate photos of yourself or of other people (even if it's just a joke)
- Treat other people online with respect and care
- Tell a parent if anyone ever bullies you, or says something to you that is not ok to say.

TOP TIP

Use a digital contract with your kids, to help set clear rules about their social media/gaming use. A contract also encourages kids to be accountable for their actions online.

PARENTAL CONTROL TOOLS

Implementing parental controls is the most pain-free and effective way of managing your child's online activity. These tools can help parents:

- Set technology to turn off at bedtime
- Keep kids off social media during homework time
- Protect kids from seeing inappropriate content
- Give you control over the apps that kids are accessing
- Manage your child's device in and outside of home
- Receive information about dangerous apps to block

WANT US IN YOUR HOME? (....wait, what?)

We've partnered with Family Zone, Australia's leading parental control tool, to give you our expertise in your home. Want us to tell you all the things you need to know about the apps your kids are using? Visit the link for more information and try it out for free: www.familyzone.com/ysafe

ySafe

Instagram

Instagram is a popular social photo-sharing app that is a fan favourite for kids ageing 8-17 (yes, you read correctly, kids as young as 8!).

Instagram is a popular platform for cyber bullying, inappropriate photo sharing, and hosts a substantial amount of easy-to-come-across pornography.

When setting up your child's instragram account, make sure the following settings are in place.

TURNING ON PRIVACY SETTINGS

1. Login in to profile
2. Click on Profile Tab
3. Click the Settings Tab
4. Click 'Private Account'

BLOCKING MEAN COMMENTS

1. Open Instagram app
2. Click on the profile tab (the icon of a head & shoulders)
3.. Click the Settings Tab (the gear in the right hand corner)
4. Scroll down and click 'Comments'
5. Click 'Hide Inappropriate Comments'

WHAT PARENTS NEED TO KNOW

Kids often have more than one Instagram account. They have one they show their parents, and one that they show their friends. Search their name or nickname in the Instagram app to try and find their additional profiles.

ySafe

SnapChat

SnapChat is a photo and video sharing app that allows you to send information that is time-limited. Kids send photos or videos that can only be accessed for between 1-10 seconds after it has been opened.

KIds can also private message and make phone calls on SnapChat. Once a message has been opened though, the message is deleted, making it impossible for parents to supervise discussions.

TURNING ON PRIVACY SETTINGS

1. When opening the app, slide the screen down with your finger
2. In the top right hand corner, click on the Settings button (the gear)
3. Under the 'Who Can...' section, set everything to 'My Friends'
4. Click on 'See me in Quick Add' and turn off

WATCH OUT...

Be careful if your child downloads the app 'Yellow'. It is linked to SnapChat and is the Tinder-equivalent for teenagers and kids. Use parental control tools to block this app.

YouTube

Kids as young as 6 are posting videos of themselves on YouTube. There are serious safety issues associated with this, as well as many people in the YouTube community that feel that it is appropriate to post horrifically mean comments to people.

WHEN POSTING VIDEOS

Before your child posts a video, make sure that comments on their video are disabled. This will stop people from 'trolling' or writing nasty comments on their posts.

ySafe

Facebook

Facebook is less popular with kids and teenagers, as their parents now have a strong presence on this platform.

One of the major problems with Facebook is their Live Feed. People can post live videos on their Facebook pages, which can sometimes involve risque or inappropriate content. Once kids have seen this though, the damage is done.

TURNING ON PRIVACY SETTINGS (settle in, this will take a while)

1. In the app, click on the 3 lines in the bottom right hand corner
2. Scroll to the bottom and click 'Privacy Shortcuts'
3. Click 'Who can see my stuff?' and set to 'Friends'
4. Click 'More Settings'
5. Click on 'Privacy'
6. Under 'Who can see the people and lists you follow', select 'Friends'
7. Click 'Limit the audience for posts you've shared..' and click 'Limit Old Posts'
8. Click on 'Reviews posts that friends tag you in before they appear on your Timeline?' and select 'On'
9. Click 'Who can see posts you've been tagged in on your Timeline?' and select 'Friends'
10. Click on 'Who can see what others post on your Timeline' and select 'Friends'

Did you complete Step 7? Your privacy settings will be pointless unless you have done this (for adults included, maybe check your own settings while you're in the swing of things?)

ySafe

musical.ly

A popular app with primary school aged children, this app allows people to film themselves signing along to their favourite song, and posting it online like their very own music video. Sounds great, right?

It is great, except for the major privacy issues and bad people ruining it for kids. This app is rife with predators, and given that videos can be geotagged (allowing people to track someone's location), if unsupervised this app is extremely dangerous for kids.

TURNING ON PRIVACY SETTINGS

1. In the app, click on the head & shoulders icon (right hand corner)
2. In the top right hand corner, click the settings button (gear icon)
3. Click 'Settings'
4. Turn on 'Only friends can direct.ly me'
5. Tun on 'Hide location info'
6. Turn on 'Private account'
7. Go back to profile page, and click 'Edit Profile'. Ensure that your child has not recorded any personal information in their bio.

ONGOING SUPERVISION

For kids on this app, only viewing other people's videos minimises safety risks (not entirely, but at least the risk of posting personal information online). However, ongoing supervision on this app is key! If your child is posting videos to their profiles, check these regularly, and delete any that are not appropriate or safe.

AGE RECOMMENDATION?

Kids all of ages love posting on this app. Even 6 year olds are loving positing to this platform! Though, to play devil's advocate, we recommend kids aged 12+ on this app (with ongoing supervision). The risks are just too great for anyone younger.

ySafe

STEP-BY-STEP

SETTING UP YOUR CYBER SAFE HOME

STEP 1.

Setup your child's devices with restrictions and settings

At the most basic level, setup filtering systems on your child's devices. On an IOS device (Apple), go to Settings > General > Restrictions, and turn on relevant restrictions (keep in mind, these are only basic functions, but better than nothing!)

Use parental control tools to block apps, inappropriate content, set up times schedules, control devices remotely, and monitor child's use. For this, we recommend using Family Zone. (Visit familyzone.com for more information)

STEP 2.

Discuss and sign a digital agreement

Use this moment to go over your expectations abouttheir use, your rules and what happens when they break the rules

This is your time to assert that you're the parent. You are going to supervise and check in when you feel itis necessary.

STEP 3.

Setup your child's accounts

Jointly create passwords

Reiterate your expectations of their online behaviour, the rules around use and your stance of supervising them

Ensure privacy settings are at the maximum level, and turn off geolocation services on their devices (for apps that don't require it, apps like Pokemon Go need this function turned on)

STEP-BY-STEP

SETTING UP YOUR CYBER SAFE HOME

STEP 4.

Make a technology-use schedule & identify a technology free-zone

In the schedule, include social activities, time online, family time, bedtime, etc. Kids work best when they have structured boundaries to help guide their expectations. This is a key factor in behaviour management.

Designate an area in the home that is ‘technology free’, like the dinner table or the living room. Keep in mind, this rule has to apply to parents too! (#positivemodelling)

STEP 5.

Supervise & participate

Check social media profiles regularly. Perform 'culls' on your child's friends or follow lists sporadically.

Use device restriction as form of behaviour management (or more free time on devices as a reward for good behaviour)

.

Make cyber safety a regular talking point in your home

.

CYBER SAFETY CONVERSATION STARTERS

How do you know who is seeing the information that your posting online?

.

How would you like people to treat you when you’re online? How do you think you should treat others online?

Get a piece of paper and draw two columns. In each column, write down what kind of personal information is and isn’t ok to post online.

What are three positive and three negative points about using social media?

When you post something online, where does it go? Can you track where that information goes once it’s online?

.Why is it important for everyone to have their social media profiles set to private? What are privacy settings and what do they do?