



YOUR INTERNET SAFETY GUIDE

BY

Dr. Maureen Griffin
Forensic Psychologist

in association with **laya** proudly part of **AIG**
healthcare

Introduction

by Forensic Psychologist, Dr. Maureen Griffin.

Dear Readers,

We are living in interesting times, it is the age of information, the digital age, the internet age, a time when technology is available to a younger and younger audience. While this knowledge can empower us, many of you are worried about the impact this technology and knowledge is having on our children.

This guide is full of advice and resources on some of the most common topics I am asked by students, teachers and parents in Schools across Ireland. As we navigate this age, we must teach our children the skills that they need so that they can reap the benefits of this technology while also equipping them to deal with the risks and dangers they may encounter.

In keeping with the theme for Safer Internet Day 2018 “Create, Connect and Share Respect: A better internet starts with you”, we have created this Internet Safety Guide.



Dr. Maureen Griffin

is a Forensic Psychologist who specialised in the assessment of internet sex offenders. She lectures on Forensic Psychology and Criminal Behaviour courses in Universities across Ireland and has worked with An Garda Síochána and the Irish Defence Forces. She has visited over 700 schools across Ireland speaking with students, staff and parents about social media and online safety.

For more articles visit www.layahealthcare.ie/thrive

1

5 tips to keep your kids safe online

2

What to do if your child is a victim of cyberbullying

3

Must have conversations to have with your kids on social media

4

Managing Screen time during holidays

5

Why we need to talk about sexting

5 Tips to keep your kids safe online



Here are five main tips to keep your kids safe online

1 INVOLVEMENT

Be involved in your child's online life. Discuss safety online the same way as you would discuss safety in real life. Watch for changes in your child's general mood and behavior when online; a change may indicate that something is happening in their online life (e.g. bullying, harassment, intimidation, access to age inappropriate content). Make sure your child knows that they can come to you if anything happens online that upsets them/scares them/worries them.

2 BOUNDARIES

Set rules/limits on what your child can do online/when they can use technology etc. For instance, **'no technology in the bedroom at night-time'**, **'no devices at the dinner table'**. Simple rules like this teach children that technology has a place within our lives and does not, or should not, rule our lives. Keep control of the modem. Check with your provider, you may be able to put time limits on for certain devices; so, there is no more **'5 more minutes'** it just times out/turns off. Some families I have spoken to are opting for a technology free day in the week - **'Tech Free Tuesday'** or **'Tech Free Thursday'** - for all members of the family.

Setting out a **'device contract or agreement'** is also handy for younger children, be it for a phone, iPad, iPod, Xbox, PlayStation etc. In this contract, you can outline what you expect from your child, what they can expect from you (e.g. it's your right to spot check/know passwords) and any sanctions you want to put in place. You can also use this contract to prepare your child for situations they may find themselves in online (e.g. what to do if they get a message from someone they do not know). Having the child involved in making the rules means they are more likely to comply.



5 Tips to keep your kids safe online

3 MODEL GOOD PRACTICES.

It is all well and good to advise our children about safe and appropriate use of technology and social media but if we do not practice what we preach, our advice is often ignored. It should not be a case of ***“Do as I say, not as I do”*** when it comes to social media and technology use. It is important that we, as parents, lead by example and model good practices for our children; manners online and appropriate use of technology should be for everyone in the family.

4 KNOWLEDGE

There is always a certain degree of worry when a new App appears –Snapchat, YikYak, ooVoo –and how it could be used to bully/harasses/groom etc. Parents can stay up to speed with new apps and sites by checking out sites like **Common Sense Media** which offers reviews of new sites/apps/games etc. Parents should have the password for all App downloads, so that you can check out the App before installing it on your child’s device. Be mindful that some children are hiding their Apps in folders on their home screen so that parents won’t immediately see the icon! Also watch for multiple accounts, often set up to avoid parental monitoring.

Some parents are very active online, speak to them, get them to show you the ropes. Know your child’s online friends and followers. Ask questions about them, just as you would ask questions about their friends in real life. This might seem daunting when they have hundreds if not thousands of friends or followers online. The reality is that they possibly only talk to/check up on twenty or thirty of these. So know these ones; they are the ones that can have an influence on your child, be it positive or negative.

5 SECURITY

Use an internet security suite, which includes firewall, antispyware etc. on all devices. For younger children (national school level), our focus should be on ***‘avoiding online risks’***, so enable parental controls and filtering on devices they are using. Know their account details for sites/Apps they are using.

As our children get older (secondary school level) our focus shifts to ***‘managing online risks’***, so go through their security and privacy settings with them, show them how to block/report etc. Advise your child not to share passwords for their devices/accounts, even with their best friends.

Children, like adults, often just tick the box when setting up an account, failing to read the T&C’s. Explain the T&C’s for the sites/Apps they are using (e.g. how long their data will be stored, who it is shared with). They will thank you for it, even if they tell you they already know!

Advice on what to do if your child is a victim of cyber bullying

Firstly, **confirm** that it is cyber-bullying. You may come across nasty messages on your child's phone or on their social media account and this could be an argument between friends, who have since made up. Make time every day to **'talk about their day'** and watch for signs that something may be wrong (e.g. changes in mood and behavior).

If your child is being cyber-bullied, remain calm. Show your child that this can be dealt with in a way that does not involve online retaliation. As social media has become an extension of our children's day to day lives, a nasty comment or text can be devastating for them. Don't diminish their sense of devastation. Understand that by

telling your child **'don't use that site or App anymore'** they are effectively being punished for being bullied. Moreover, not using a particular site or App, does not guarantee they will not be bullied, as your child does not need to be on a particular site or App to be targeted on it.

Do not fight back on your child's behalf. Even though every bit of you may want to write back a smart comment or encourage your child to do the same, this will only add fuel to the fire. Furthermore, it will not teach your child how to deal with conflict situations in the future. Bullies are looking for a reaction (i.e. upset, anger, fear) and giving them one can escalate the situation.



Advice on what to do if your child is a victim of cyber bullying

INSTEAD ENCOURAGE YOUR CHILD TO STICK UP FOR THEMSELVES BY;

- 1. Blocking and/or removing** the person as a friend/follower. Children should also be encouraged to stand up for what is right online and block individuals they see bullying/abusing others, even if they themselves are not directly affected. If there is no audience, then there is no show;
- 2. Reporting the issue** to the site/App/phone company etc. as applicable;
- 3. In some cases, approaching the person** in real life (if known in the neighbourhood/school etc.) can also help the child stick up for themselves. This works especially well at National School level, where the child can let the bully know that what they did/said online was not okay. This can be quite therapeutic for both target and bully, and often they remain friends afterwards. Depending on the circumstances, parents may also wish to **talk to the parents** of the child/children that are involved in the bullying;
- 4.** Advise your child to **take screen shots** of the cyber-bullying. This will serve as evidence of what has happened and may be needed by the school or Gardaí.

Parents should link in with the school and let them know what is happening. Although cyber-bullying happens outside of school, it tends to seep into school, particularly when the children involved attend the same school. Let the principal and class teachers know what is going on, so they can monitor and/or deal with the situation from a school standpoint. In September 2013, the Department published their **Anti-Bullying Procedures for Primary and Post Primary Schools**, requiring all schools to have an anti-bullying policy (including cyber-bullying) within the framework of their overall code of behaviour. If, as a parent, you feel the issue is not resolved by the school, you can report to the schools Board of Management. The Department of Education and Skills do not investigate complaints but can advise parents on how to proceed if necessary.

For more serious cases such as those involving persistent harassment, sexually inappropriate content and/or contact online, abuse/harassment/grooming by an adult etc. parents should contact the Gardaí.

If there is content online that is being used to bully/harass your child –for instance a fake account containing pictures/videos of your child –you will need to contact the site/App and request that that content be removed. If you are

having trouble getting content removed, you may wish to contact **'The Hit Team'** a privacy consulting firm who assist individuals who have suffered from an online infringement. As the saying goes **'prevention is better than cure'**, so do not wait for something to happen before discussing cyber-bullying with your child. Unfortunately, there is no fool proof way to guarantee that your child will not be upset/annoyed/bullied/frightened at one point or another online. Even completely removing technology from their lives does not guarantee they will not fall prey to online bullying; as one of the more sinister things about cyber-bullying is that you do not need to be using technology to be targeted online.

Nonetheless, as parents, we can help prepare our children for situations they may find themselves in online. Have regular chats with your child about their online life –what sites they are using, who they are following, what they like/dislike etc. Use examples from the media to open discussions. Ask questions such as **'has that ever happened to you, or a friend?'** **'what would you do if that happened to you?'** Be mindful that your child can just as likely be a cyber-bully or bystander, as a victim of cyber-bullying. Discuss the various roles involved in cyber-bullying and ensure they understand the impact and consequences for all involved.

Conversations to have with kids if they are using social media



Social media can be daunting for many parents. With new Apps and sites emerging daily, we as parents can often struggle to keep ahead of our 'digital native' children.

Regardless of the social media site or app your child is using, here are 5 conversations you should have with them.

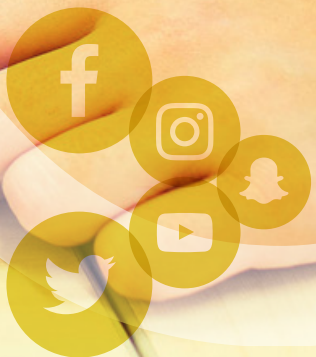
WHAT IS THE MEANING OF 'PRIVACY' ONLINE?

What does it really mean when we select '**private account**'? Once we have selected this option, can we then share whatever we want and it will remain private? Unfortunately, this is not the case. The privacy option on most sites means that our information is a little less public, only shared with friends/followers we accept. However, profile pictures, bios and usernames can remain public. Once we share content online, we lose control of that content. It can be copied, shared and edited by anyone we share it with. From speaking with young people across Ireland a statement I hear a lot is **"I have 800+ friends/followers..... but my account is private"**. As parents, we must challenge this belief.

WHO SHOULD WE ACCEPT AS FRIENDS/FOLLOWERS ONLINE?

Most young people I speak to admit to having friends or followers online that they do not know in real life. This is not always negative or risky but all it takes is accepting one unknown individual whose intentions are destructive. The number of friends/followers remains a popularity contest, with young people accepting strangers to look '**cool**', get more '**likes**' and have more '**streaks**' (this is where you and your friend have '**snapped**' each other but not chatted within 24 hours for more than three consecutive days). This idea currently dominates our children's lives and is often seen as a way of quantifying friendships. Discuss what it means to be a friend and how friendship **cannot** be simply measured by a snapchat emoji or streak score.

Most young people also admit that they have friends/followers they never speak to –they merely accept them to '**creep**' on their account. By accepting someone as a friend/follower you allow them access to the content you are sharing, ultimately allowing them to '**creep**' on you. Talk to your child about customising their



Conversations to have with kids if they are using social media

settings, so they can still maintain their friends list, but choose who to share content such as pictures etc. with. In real life, we would never hand over the volume of information we hand over when accepting a friend online. Young people think it would be 'weird' if someone asked them in real life ***"Will you be my friend? Can I have pictures of you, your snapchat username, a list of your friends etc."***

They would never hand over that content in real life yet that is exactly what they are doing when they accept someone as a friend or follower online. Help break down the distance technology creates by talking about the reality of accepting friends/followers and how much content they are handing over.

HOW TO PROTECT OUR MENTAL HEALTH ONLINE

Online we subject our mental health to pressures we would never subject it to in real life. I doubt any young person would stand outside their house with a box of selfies, holding them up to random strangers as they pass and asking them if they ***'like'*** this picture or if they would like to comment on it. Yet online, our children seek approval, validation and appreciation from strangers daily. While amazing positives can

be gained from self-expression online, negative comments, dislikes and disapproval can have a damaging effect on our children's developing self-esteem. If left unchecked this can result in mental health difficulties such as anxiety, depression, self-harm, eating disorders etc. I repeatedly meet young people who will not leave an image on their account online unless it receives a certain amount of ***'likes'***. Have a conversation with your child about what they share online and what they expect by sharing (e.g. likes, comments, more friends/followers). Discuss whose opinions online matter to them and why.

WHAT IS THE ROLE OF THE BYSTANDER?

As parents, we all worry that our child will be bullied but very few of us worry that our child will be a bully or a bystander. These are roles we need to talk about. Most children, like us as adults, share, like and comment on images, videos and posts online, often without thinking of the consequences of those actions. By sharing, liking and commenting we are creating a larger audience for the content. So, while your child may not be the bully, they may be assisting bullying by sharing, liking and commenting.

HOW TO ACHIEVE A HEALTHY BALANCE

Like most things in life, moderation is key when it comes to social media. Young people often gasp at the thought of a ***'social media fast'***, panicking about ***'losing their streaks'***.

However, they also often admit, they feel less stress, less pressure and less anxious, when they give technology a break. Set simple rules that suit your family – for instance, no devices in bedrooms at night-time, no devices at the dinner table. We need to teach our children and young people to give technology a place within their lives. Talk to your child about times when it is inappropriate and/or unsocial to use their devices. Discuss when is okay and **not okay** to take pictures/videos.

Model good practices and teach your child that sometimes trying to capture everything with our devices means we often miss what is right in front of us.

How to manage your children's screen time

How much screen time is too much?

Many parents are concerned about how much time their children are spending in front of screens. So how much is too much? How can we control it?

The American Paediatric Association (APA, 2016), recommends unplugged playtime for infants and toddlers (i.e. no screens) and a limit of 1-hour high quality programming for 2-5 year olds, with active parental involvement.

For children aged 6 and older, they recommend limiting the amount of screen time so as to allow for adequate physical activity, sleep, play etc. As not all screen time is equal, it is important that we pay attention to **what** our children are doing online; instead of solely focusing on a specific amount of time (e.g. are they passively watching shows; playing interactive games with friends; video chatting with family/friends/strangers; creating videos/music).

To support the APA's new recommendations, they have published an online tool that allows families to create their own personalised **Family Media Use Plan**. Devising such a plan as a family, can greatly help in getting an appropriate balance between screen time and other activities, especially during the summer months.

The APA also provide a **Media Time Calculator** which helps families determine the most appropriate amount of screen time for children in different age brackets - from 18 months to 18 years. Each age bracket is set with the recommended amount of time for sleep and physical activity, allowing the user to add time in for additional categories such as school, homework, family time, meals, reading, free time etc.





How to manage your children's screen time

As parents, we play a crucial role in setting good examples for our children when it comes to social media usage and screen time. By creating a Family Media Use Plan, we can set clear expectations and boundaries for everyone in the family, unique to the specific requirements of each individual family member.

In addition to modelling good practices and creating a family plan, here are three things to be mindful of.

1. MAINTAIN GOOD HABITS

Don't undo good habits built up during the school year. For instance, letting devices creep into bedrooms while children are off school. The World Health Organisation, Safe Foods, and the National Sleep Foundation, have consistently demonstrated the negative health effects of having technology in bedrooms and/or using technology as a sleep aid (i.e. increased likelihood of developing childhood obesity/diabetes in later life; reduction in the amount of sleep, quality of sleep and day time alertness). **Recent research** has also indicated that increased night-time mobile phone use is

directly associated with increased externalizing behaviour, and decreased self-esteem and coping. Despite this, the clear majority of students I speak with, who have devices in their rooms at night; admit they receive messages after midnight. It is therefore vital that we maintain bedrooms as screen free zones, all year round.

2. BE WITH THE ONES YOU ARE WITH

Children, and adults alike, often admit that when they visit a friends' house, one of the first things they do is ask for the WIFI password. While acknowledging all the amazing benefits of technology and the role social media plays in our children's lives, we need to remind our children to ***be present, to be with the people they are with.***

Although our children are connected 24/7 and in constant contact with their friends, they often maintain such contact in a very disconnected way - without making eye contact, without speaking, without picking up on behavioural cues/emotions.



How to manage your children's screen time

Talk to your child about the importance of true meaningful connections with friends. Friendship is more than maintaining a **'streak'** on Snapchat and more than someone who will **'like'** your pictures. When their friends call over, remind your child to be present. Set aside time to be connected in real life, instead of constantly multitasking with devices. Identify **'device-free times'** that work for you as a family (e.g. when eating, driving, walking, visiting grandparents) Some parents control screen time by changing WIFI passwords on a daily basis and only handing it over when children have earned their screen time by completing tasks in other important areas (e.g. physical activity, chores, reading).

The **Screen Time App** may also be of use to parents who wish to limit the amount of time their children spend online. This App allows you to set time limits for your child's device from your own phone (or browser); enable restrictions for specific Apps; pause your child's online activity and assign tasks that must be completed to gain screen time. It also sends parents daily summaries outlining which websites and Apps their child used and for how long.

3. HOLIDAYS AND SHARING

If you are going away, either here in Ireland or abroad, wait until you are home again to share all your adventures. Burglars have been known to use social media to identify empty houses, especially during holiday seasons. Talk to your children about their location settings, which can be enabled/disabled for individual apps they are using. Although children tell me **"it's not safe to share your home address"**, a lot admit they have location setting enabled for a chatting App or social networking site. As most of their messages are sent from home, they can be inadvertently sharing their home address.

Also, talk to children about what is okay/not okay to share while away on holidays. It is much easier to have a discussion on **'why NOT to take a picture of mammy/daddy in their bikini/Speedos'** in advance, instead of having to claw back that image when it has been shared online.



Sexting, what parents need to know



‘Sexting’ or ‘sex texting’ refers to sending sexually explicit messages, images and/or videos via digital means. Primarily such ‘sexts’ are sent using mobile phones and/or social messaging applications such as Snapchat, Viber and WhatsApp etc.

You may have heard of high profile sexting cases over the years, such as that of golfer Tiger Woods or American Politician Anthony Weiner. Each week we read about a celebrity who’s imitate pictures have now been leaked; coincidentally often just as their careers are failing! This sets a culture where sexting is seen as the norm among young adults and even children.

SCALE OF THE PROBLEM

From my experience, having visited over 600 schools across Ireland, Irish children are very aware of the phenomenon of sexting. Consistent with international research from Australia, USA and the UK, sexting is more common among secondary school children than primary school children. However, I have been made aware of cases in Ireland where children as young as 10 years of age have engaged in sexting.

WHY DO CHILDREN ENGAGE IN SEXTING?

There are many reasons why children engage in sexting. The following are some of the main ones I have observed;

Due to pressure from a boyfriend/girlfriend/ friends or as a means of demonstrating commitment in a relationship – where they often believe it will be kept private;

Imitating celebrities that they may follow on sites such as Twitter or Instagram etc.;

To show off or get attention (e.g. **‘selfies’** or **‘belfies’**);

To entice someone or flirt;

Groomed by an adult;

Due to exposure to pornography online, where such images become normalised and thus contribute to the sharing or demanding of self-generated images.



Sexting, what parents need to know

WHAT DO PARENTS NEED TO BE AWARE OF?

As children are not neurologically equal to adults (decision making, judgement, impulse control etc. are still maturing), it can be difficult for them to grasp the long-term consequences of their often-impulsive actions. As parents, we need to teach our children how to take responsibility for their actions.

Have open conversations about personal responsibility, boundaries and how to deal with peer pressure. Such conversations should occur throughout children's lives and not just when an issue arises;

Explain that once they send something online/through their devices they lose control of that material -it can be copied, printed out in real life, shared on other sites and with other people. In recent years, there has been a dramatic increase in the amount of 'revenge porn sites' hosting sexts;

Outline the consequences of sexting, both legal and psychological. Sending sexts can harm their dignity and reputation and potentially affect job and college prospects. Use case examples that they can relate to (e.g. the case of Jessica Logan in Cincinnati, Ohio, the film *'Sexting in Suburbia'*, 2012, PG-13 and the MTV series

'Sexting in America: When Privates go Public', R13); Encourage your child to count to five before they hit send and employ the *'Nana Rule'* when sharing online; what actions and decisions would you make if your grandmother was standing right behind you?

WHAT SHOULD YOU DO IF YOUR CHILD HAS SENT A SEXT?

Find out why this message was sent. As indicated above the reasons people send sexts differ; was it within a romantic relationship, was it sent impulsively, was it sent out of revenge after a relationship ended, was the young person forced?;

Depending on the reason the message was sent and the age/s of the individual/s involved the Gardaí may need to be notified (i.e. in the case of an adult forcing a minor);

If the recipient of the message is a friend of the young person, the young person should ask them, in person, to delete the message;

If the message has been sent online, contact the website to have the image removed;

Support your child as they deal with the psychological effects of knowing their image is *'out there'*

WHAT SHOULD YOU DO IF YOUR CHILD RECEIVES A SEXT?

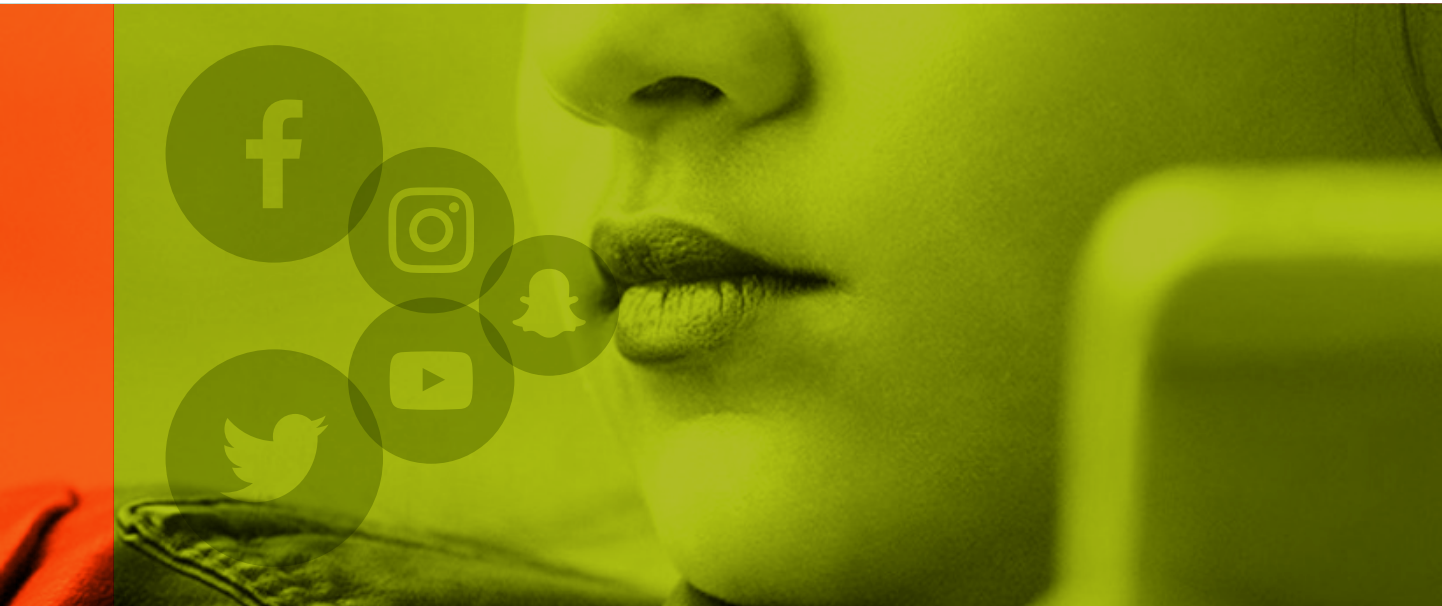
Firstly, commend your child for coming forward and telling you about it; they have done the right thing; if possible establish who sent the message - a friend, girlfriend, boyfriend, stranger;

Depending on the age/s of the individual/s involved the Gardaí may need to be notified (i.e. in the case of an adult sending material to a minor);

If the sender is a stranger, advise your child not to respond and block the sender. You can report sexually explicit and/or distressing pictures you receive to Hotline.ie, an anonymous facility run by the Internet Service Providers Association of Ireland **www.hotline.ie**

If the sender is a friend of your child's, you should contact their parents so they can talk to their child;

Make sure your child does not forward the message to anyone else or share it through any other digital means.



We hope that you found this guide useful,
please share it with your friends and family.
For more up to date news on health, lifestyle,
family articles and member stories please visit
www.layahealthcare.ie/thrive

laya
healthcare proudly part of **AIG**