PARENTS KEEPING CHILDREN SAFE ONLINE.

DETECTIVE SERGEANT MARK MOORHOUSE.

SUPERVISOR HAWKES BAY CHILD PROTECTION AND ADULT SEXUAL ASSAULT TEAM.
WHAT ARE THE ISSUES ???

- Sexting and the link to Extortion and Bullying Tactics.
- Dangers of introduction to Sexual Activity, Bullying and Emotional Harm/Suicide.
- Snapchat and how unsecure it really is. Snapchat - Repost - screenshot - cameras on smartphones and apps to screenshot.
- Murder Sex Case and how easy the access was.
- Increase in Sexualised Behaviours by Children at School.
- Access to WIFI and Data, Increase in WIFI Hotspots versus education.
- Increase in Social Networking Sites - High School Case and Bucket List.
- Risk getting information from Porn Creates.
- Latest Pornography being made is going to be Virtual reality.
- Accepted Behaviour Norms Changing.
- Move towards Educators being provided with the tools to give Children and Young People healthy options other than Porn for Info.
Let's first discuss the issue of addiction to the device itself.
TEN POINTS TO KEEPING CHILDREN AND YOUNG PEOPLE SAFE ONLINE.
1. COMMUNICATION:

- Talk to your child early and often about e-safety.
- Just like any other life lesson, clear and simple communication is key with young children.
- The earlier you begin this process the better.
- Keep your conversations short but regular, rather than long and occasional.
- This will make it much easier for young children to digest, and means that online safety has a better chance of being accepted as ‘normal’ and something that they won’t feel sensitive about.
- Encourage young children to remember the lessons you teach, and clearly and positively acknowledge their ability to successfully remember them.
2. ENQUIRY:

- Take an interest in what your child does online
- Young children enjoy the attention of their parents and teachers, no matter what activity they undertake.
- This is also true of their participation in the online world. Begin by asking questions such as “Which websites do you like spending time on?”, “What are your favourite things to do on these websites?”, “Which are the websites you would recommend to your friends?”, “What are your favourite online games?”, and “Who do you play these games with?”
- Actively enquire about the specifics of what they do and have achieved online, remembering to demonstrate positive reinforcement and encouragement. Create an environment of trust which encourages your child to voluntarily share their online experiences.
3. DEMONSTRATION:

- Let your child show you how to participate in their online world.
- As with gaining attention and approval, young children enjoy the opportunity to demonstrate their skills and experiences to teachers and parents. With the amount of time they spend online, the chances are your child may well know more than you do about the online world.
- This is to your advantage, since it will enable you to better understand exactly what they know and how they do it, and as a consequence determine what controls need to be put in place for their protection, if appropriate.
4. ASSISTANCE:

- Ask your child to help you in the online environment.
- What better way of discovering how your child thinks and behaves online than asking them to help you with online safety sensitive tasks?
- Activities such as creating a social media profile, setting up an email account, and how to ‘friend’ someone will provide you with the insight you need to determine whether they are adhering to online safety good practice.
- They don’t need to know that you actually might already know, but by getting them to show you a parent can learn a lot.
5. INTELLIGENCE:

- Learn who your child talks to online
- With so many people intentionally misrepresenting themselves online, it's vital to keep tabs on who your child communicates with in the digital world. Unfortunately, children do not perceive people they meet on the internet as strangers, rather they see them unreservedly as online friends. For this reason, it is vital for parents to keep track of who their child is talking to.
- As with Enquiry and Assistance, taking an interest in a child's friends can reveal if they are vulnerable to exploitation.
  - “Who do you know that has the most online friends?”
  - “How can (that person) know so many people?”
  - “How do you choose who to become friends with online?”
- This should provide you with an insight into your child's attitude to online safety, and whether their behaviour needs to be addressed.
- If appropriate, explain to your child just how easy it is for people to lie about themselves online.
- If necessary, consider creating a false profile yourself and ‘friending’ your child. This will allow you to demonstrate to them just how easy it is to be deceived online.
6. LIMITATIONS:

- If appropriate, set boundaries and agree rules.
- Setting internet usage rules and boundaries can only be determined by each individual child’s age, experience and attitude to online safety. Whatever they may be it is vital to explain why they are in place. If your child does not understand their importance and relevance they are likely to ignore them and attempt to conceal their online activities from you.
- Set Time Frames around the amount of time your child is allowed to spend online.
- Set the times of the day that they are permitted to go online based on commitment to other activities.
- Children will play the privacy card on many occasions so care around internet access in the privacy of their room is a matter to be cautious of and discussed as part of the conditions of access.
- Parental controls around internet access and access to content are available on the NetSafe.govt.nz Website. Internet Providers also can provide tools for online safety as well.
- Stats Indicate an average of 5-6 hours a day online for most young people.
- If you have a child that enjoys playing games online be sure to check the age rating of any and all games before they are given permission to play.
- Insist that your child informs you of who they’re playing with.
- Online Predators game with children and young people online and have been known to lure them into chat rooms.
7. APPROPRIATENESS:

- Ensure your child only views content that reflects their age.
- At the end of the day, parents know their child best. There’s no ‘one size fits all’ solution to determining what is appropriate for your child to view.
- Ensure your child is not exposed to inappropriate content whenever possible.
- By following the previous online safety tips, parents should be able to obtain a good understanding of which websites and online activities their children actively participate in.
- Parents can also monitor browser histories and should do so. Do Not .
- If your child’s access to the internet is through a shared device (such as a family desktop or laptop computer, or tablet) you should ensure that the homepage of your browser of choice (the first page that appears when you open an internet window) is appropriately set for your child to see.
- Creating individual user profiles on your digital device allows parents to set specific limitations and restrictions that are only applied to the designated profile user.
- Parental controls can also help you to limit what your child sees online, and privacy controls can limit the exposure of personal information, ensuring that it stays private.
- In the digital classroom, many teachers retain control of what their children and young people can view by utilising classroom management software blocking, filtering and monitoring features.
8. CONTROL:

- Use parental controls to filter, restrict, monitor and report.
- With older children, particularly teenagers, parents may encounter more resistance to perceived interference and intrusion.
- Parental controls are readily available to filter and restrict access to content.
- Parent’s can even review online activity and generate reports.
- There are a variety of ways parental controls can be employed to ensure your child’s online safety, which can be found throughout the different tools necessary to access the internet.
- First off, the device you access the internet with will have parental controls. Desktop computers, laptops, tablets, smartphones and games consoles all have settings to activate parental controls.
- Next, your connection to the internet will provide parental controls. All the leading the ISPs - Internet Service Providers - provide a suite of parental controls as standard, allowing parents to restrict internet access and filter content.
There is specialist software designed to filter, restrict and monitor internet usage. These are very popular and are becoming more prevalent throughout all aspects of online usage.

Classroom monitoring features are now perceived by children and young people with access to the digital classroom as the norm.

It is not a giant leap for youngsters to accept this level of control in the home if their access is already subject to filtering, restrictions and monitoring.

One important thing to remember is that parental controls ONLY apply to devices, services and software that you directly have access to.

They do not apply outside of this limitation, such as when your child accesses the internet via public Wi-Fi, or when at a friend’s home, or in the digital classroom.

If the preceding online safety tips have been followed, and trust established, it is advisable for parents to talk with their child about how and where they use public Wi-Fi, and what they are and are not allowed to do online outside of the family home. You should also consider liaising directly with other parents about setting strict boundaries regarding what your child can and cannot access online while within their home.
9. PRIVACY:

- Protect your child’s personal information.
- Remember everybody is vulnerable to attacks on their personal information.
- While it is vital that parents take the lead in establishing control of their child’s privacy settings, the truth is that many adults fail to adequately protect themselves, or even understand the motivations and consequences of private data collection.
- By default most online privacy settings will be set-up to favour the service provider. High profile examples like Facebook and Google are run on business models which depend on extracting as much personal user data as possible, for the purpose of assisting advertisers when targeting customers.
- It’s part of the fine print when people sign up to these Social Media Sites.
If you’ve ever signed up for anything online (and provided your email address) the chances are (if you check your email inbox) you’ll have noticed that you suddenly received a flurry of unsolicited messages from businesses trying to sell to you. It’s not a coincidence.

These, and many other data gathering activities, leave children vulnerable to invasions of privacy.

In all likelihood they may not conceive the notion that they are being tempted by offers and prizes purely for the purpose of data gathering.

It is important for parents to discuss this issue with their child as early as possible, so as to indoctrinate them with the knowledge necessary to protect their privacy.

Parents should consider instructing their child around taking great care around the online use of their personal information.

Parents may even wish to insist on censoring the type of photos their child posts or shares of themselves online.
10. REPORTING:

- Instilling confidence in your child to deal with online safety concerns.
- Parents know that children will often conceal problems from them which originate in all aspects of their lives.
- It’s no different when issues arise from experiences on the internet.
- Unfortunately, the consequences of concealing problems arising from negative online experiences, such as cyberbullying, threatening behaviour, child grooming, unregulated advice and debt accumulation can have tragic consequences.
- While there is no single fix that works for all families – every child/parent relationship is different – there are safeguards and advice that parents can instil in their child that can minimise the potential consequences of negative online experiences.
- Many online applications, particularly social media platforms, have reporting functions that allow users to communicate their concerns and grievances to service providers.
- Parents should always make it clear to their child that they should come to them first (or a pre-agreed, trusted adult, such as a teacher or relative) if they encounter a problem online, but that in the event they feel they cannot do so be made aware of the reporting tools available online.
CONSENT WHAT DOES IT REALLY MEAN ???

CONSENT

IT'S SIMPLE AS TEA
QUESTIONS?

- Detective Sergeant Mark MOORHOUSE.
- Child Protection & Adult Sexual Assault Team Supervisor.
- Eastern District - New Zealand Police
  P +64 6 831 0366 M +64 21 191 65
  E mark.moorhouse@police.govt.nz

- Kaahore taku toa i te toa takitahi, he toa takitini – (One cannot succeed without the support of others)