

Of Digital-Birds and Cyber-Bees: Having the ‘Cybersafety Talk’ With Your Child.

When is a good time to talk with your child about the potential risks and dangers of cyber technology? The short answer is ‘yesterday’. Nowadays, children as young as two or three years of age are using online technology. It is a common proverb that it is far better to build fences at the top of cliffs rather than having ambulances available at the bottom to try and help those who have unfortunately fallen, jumped or have been pushed off the edge. This is very true for the many cliff-like areas of cyberspace that are particularly dangerous (and sometimes even life threatening). However, it must be held in balance that the Internet and Information Communication Technology (ICT, such as mobile phones) provide many wonderful benefits to all members of the community, and it is very important that we do not lose sight of this. The focus of this article is not to articulate the dangers and pitfalls (these are details are included in our website, listed the end of this article), but rather to give some important pointers and suggestions to those facing the prospect of having a ‘birds & bees’ conversation about the Internet and associated technologies with younger folk.

Talking about potential areas of danger with young people is often an uncomfortable experience for adults. We might feel that we are lecturing, nagging, and catastrophising, or we might have to talk about issues that make us uncomfortable, such as sex, violence, death and religion. Such ‘chats’ are often made worse when we do not feel knowledgeable and confident with the subject matter. Nevertheless, it is far better to err on the side of caution, and talk about issues *before* they become a problem. Ignorance is not bliss when it comes to situations that threaten your child’s safety and security.

A good place to start your conversation is simply to ask your child what they use the Internet and other ICT for. You might be surprised, and possibly shocked by their responses. Many children are far more advanced in their technological knowledge and practices than they are given credit for. We know through research and reports that quite a number of young people use the Internet in secret, and many also have mobile phones or own extra and alternative mobile phone memory cards (SIM cards) that their parents and caregivers are completely unaware of. Putting things in context, many of us can stretch our memories back to our own childhood where our parents and caregivers were remarkably unaware of what we were into, where we sneaked off to, and what we got up to. Do not underestimate your young person’s ability to lead a life online that is less than completely transparent to you.

Be aware that the young person might be surprised by, and even resistant to, your interest in their cyber-life. They may interpret your curiosity as being intrusive and controlling (a very typical adolescent response), or they might not credit you with enough brainpower to be able understand what they tell you about ‘cyber-stuff’ (and they might actually be

right!). Be honest with your answers to any questions about why you are interested. It is better not to use the stock answer of “just because”, rather let them know that they are important and loved, and that you want to keep them safe. This explanation goes some way in compensating for any possibly over zealous, over-the top or hysterical reactions that you might have to what they tell you they are getting up to!

This early stage of your conversation presents you with an opportunity to confess your actual level of understanding of all things cyber. Unless you are involved in the business of ICT, or have recently trained in computer science, there is a very real chance that you will not know as much as the young persons in your care do. Even if you do actually know more than they do *about* the technology, it is likely that you will still have less of an understanding of what young people are *doing* with it. It is also unlikely that you will be able to hold such a lead, as they grow older and wiser. Admitting your naivety and asking the young person to explain things to you to ‘teach you’, will not only make this a more informative (and honest) process, but will also even out the power differences between you and them, making it more of a discussion and less of a lecture.

When listening to the young person’s answers to your questions about what they are doing online, it should be remembered that their side of the conversation is being influenced in light of how the young person thinks that you will react to their disclosures. If they think that you will have a negative or overly strong reaction to them telling you things about their activities that you might disapprove of or be startled by, they will be less inclined to be open and honest with you. This is especially the case if they think that your automatic response to them disclosing information to you will be taking their computer or mobile phone away from them! Ask yourself if you are presenting as a parent or caregiver who is calm, rational and understanding, and therefore is approachable with a problem or concern. If the answer is ‘No’, you can either modify how you might appear to the young person, or alternatively, arrange for another trusted adult (partner, relative etc) to be the designated person for the young person to talk with about cybersafety issues. It is very important not to force your child’s cyber life ‘underground’. The reality is that they can go online somewhere else (school, a friend’s, a cyber café) or use a mobile phone you are unaware of to do what they want to do.

Having tried to ascertain what the young person is actually up to (and reserving a healthy amount of caution in light that it is reasonably ‘normal’ for young people to minimise, alter, and generally ‘adjust the truth’ on occasion for whatever reason *they* feel is justified), it would be timely to broach the subject of expectations about their cyber-usage. You will need to discuss your expectations in balance with their expectations. Prior to your discussion, you might want to have already considered (and maybe discussed with your partner) some of the following issues to be raised :

- The amount of time and money spent on the Internet, mobile phones and other ICT devices

- When and where the technologies are used and not used. For example, are mobile phones left turned on at night, can the young person use the Internet for chatting with friends before they have completed their homework, and so on.
- What the young person will do if they encounter a situation in which they feel uncomfortable or upset, or if they have done something wrong (who will they tell and how)
- What to do if they want to meet a person from cyberspace offline (face-to-face)
- What is legal and illegal online

(Remember you can find more information about such topics on our website)

You could also figure out an ‘emergency response plan’ (possibly in consultation with the young person if they are old enough). This might cover what the young person will do if they feel that they are in a situation of risk or uncertainty, how they will contact and open a discussion with you (or the designated adult), and what the boundaries will be around your response. For example, imagine that your young person is receiving sexually aggressive text messages from a person they met in a chatroom, or that they turned off the firewall on your family’s computer and have now accidentally downloaded a virus. How do they initiate a discussion with you? Is it OK if they phone you at work, wake you in the night, call you anytime? Can you agree to boundaries, such as you being open, calm and non-explosive (or try very hard to be), regardless of what they have done, and if there is to be punishment, that it *might* not necessarily include the loss of the cyber technology?

In addition, the young people will likely have expectations of you. They may require that you will try and follow what they are talking about, even if it is all foreign to you. If you feel that you need and want to know more about cybertechnology, you might consider taking a course at night school, visiting NetSafe’s website, or getting yourself some reading material (e.g. NetGuide magazine is available at all supermarkets and is a good source of information and help).

Deciding on the rules, regulations and boundaries will depend on the intellectual age and ability of the child. Special consideration should be given to how much you feel the child is able to deal with online situations on their own, especially if you feel that they are too young, or have special needs (psychological and/or physical challenges), or other factors that might make assessing risk, following instructions and communicating with you a problem.

Having discussed the young person’s online behaviours, the expectations of both parties, the rules and regulations, and what to do ‘if things go wrong’ or if they are worried, scared or concerned, finish your conversation with a clear summary of what has been raised. You might want to end with a verbal contract or agreement that you can both adhere to.

The outcomes of your continued discussions about your young person's life online (and the discussions will need to be ongoing) will also inform you about who else you will need to include in establishing and maintaining the young person's online safety. For example, the rules and guidelines that you set for your own home will need to be respected in other settings, e.g., at your child's friends' and relative's homes, and in fact, for any place that your child is and you are not. Many people who share custody of a young person do not consider the cyber access that their child has at their ex-partner's home. Keeping in touch with other adults dealing with the same issues (such as your child's friend's parents), will help ensure continuity of your arrangements and rules, and can also be a source of information and support for you. Share what you find and think. If you have concerns, you might talk with others and discuss them with the school and other parents that you know. A surprising lot of difficulty can be avoided if parents/ caregivers and teachers have a little warning (a 'heads-up') to anticipate a problem in advance.

Lastly, congratulate yourself on being proactive in your young person's cybersafety and wellbeing. Hopefully, you have established a clear and healthy communication channel, which is probably the most important fence we can put at the top of that cyber-cliff.

Nathan Gaunt
NetSafe Internet Safety Group

Email: Nathang@netsafe.org.nz Website: www.netsafe.org.nz