

13 Cybersafety tips: Parents



powered by
eSmart[®]

1. Start with an “Acceptable Use” Agreement

Children can't know all there is to know about their responsibilities and the behaviour expected of them without some guidance. Before you give them access to the internet or to a mobile phone, it's important to talk to them and provide clear rules to ensure they are being smart, safe and responsible online.

[ACMA Cybersmart - Parents](#)

2. Talk privacy and security

As a family it's good to discuss these issues regularly. Cover topics such as how many online friends is appropriate, what kind of information is ok to share online and why meeting up with someone you meet on the internet is not advisable.

[ThinkUKnow - Staying in Control](#)

3. Set safe search and security controls

Find out how to set security and privacy settings, password protect devices, and limit the kinds of content your children can search for by applying ISP level and protection software parental filters. Turn off Bluetooth, geo-locators etc. on your children's devices and explain why leaving these on is not a good idea.

[ThinkUKnow - Parental controls](#)

[Telstra - WiFi tips](#)

4. For younger children, insist on computers being used in the home's public areas

Even if you aren't constantly looking over their shoulder, it's good for children to know that you easily could help limit the opportunities for them to search for inappropriate content, or to make poor judgements online.

[ACMA Cybersmart - Parent Guide to online safety](#) (with age appropriate tips)

5. New lights out is Wi-Fi off and mobile devices charging in a central place

It's tempting for kids to keep using their devices through the night, but a lot of bullying and other poor behaviour happens late at night. It's good family policy to turn the WiFi off after a certain time each night.

Similarly, make it a rule for the whole family to surrender all their devices to a central overnight charging spot – adults too. The kids will comply more readily if they see that this is an expectation of everyone.

[ThinkUKnow - Mobiles](#)

6. Mobile plans and internet download limits

Help your child understand the impact, and costs, of over-use and help them to know how to keep track of their usage. Set limits.

[ACMA Cybersmart - Excessive use](#)

[ACMA Cybersmart - Mobile phones](#)

7. The importance of keeping software updates up-to-date

Teach your children the importance of downloading the updates to their software – not just their virus protection updates, but all software updates – but also teach them to ask you first. And yes, you should always read the terms and conditions.

[ACMA Cybersmart – ESecurity](#)

[ThinkUKnow - Protect your computer](#)

8. Teach your child to check links in emails carefully and beware of fake URLs

Some emails and links are more obviously scams than others, but lots of people make the mistake of clicking on something that has malware in it. Learn how to tell when it is safe to open an email or link.

[ThinkUKnow - Malware](#)

[ACMA Cybersmart - eSecurity](#)

[Telstra - common scams to be aware of](#)

[ACCC Scamwatch - Spam \(junk mail\) offers](#)

9. Researching online

Help your child understand that not everything online can be trusted as credible or appropriate. Guide them to some good internet search tips and search engine features.

www.kids.net.au

10. Downloading videos, images and music

Downloading of videos, images and music is illegal unless express permission is granted. Teach your children about the risks of peer-to-peer (P2P) file-sharing sites - they are virus incubators – and there is a high likelihood of your computer crashing (or slowing down). Use legal file sharing services to avoid the drama.

[Smartcopying - 'All right to copy?'](#)

[ACMA Cybersmart - dealing with offensive or illegal content](#)

11. Get involved

Get involved in the efforts of your child's school to raise awareness of cybersafety and bullying issues.

Show interest in what your child is doing online. Ask them about their online social networks and what the issues are from their point of view. This will help you identify if you need to offer extra support at any time.

[ACMA - holistic approaches to cybersafety](#)

[eSmart Schools](#)

12. Have a plan for if your child is being (cyber) bullied

It's important to talk about the possibility of bullying – both off line and on. Find out what your child's school anti-bullying policies and procedures are and discuss these – let your child know there are clear steps to take and that it's ok to report it.

[NCAB - bullying resources](#)

13. Make a formal report

If your child is feeling threatened or seen something that's disturbing – you will feel better if you start to take positive action. Show your child how to report and block - use these resources to help you.

[ACMA Cybersmart - reporting lines](#)

[ThinkUKnow - how to report](#)