

Safety tips

The safety tips draw on analysis the data gathered and available research. This section of the paper is intended to provide, in one convenient place, recommendations to parents and guardians to help them help their children have a safe, positive and valuable experience with virtual worlds.

Safety tips for parents and guardians

	#	Recommendations	Description
Safety & security of your personal computer	1.	Keep the computer in a common room	Keep the computer in a common room and be present when children use Internet. If you cannot be present, consider keeping a close watch on what your children are doing online by using a key logging programme to trace their steps online, although children may lose trust in parents who reveal use of such tools too clearly.
	2.	Install firewall and antivirus software	Ensure that your computer has a firewall and antivirus software installed. Teach your children the basics of Internet security.
Rules	3.	Set house Internet rules	As soon as children begin to use the Internet on their own, establish a list of agreed rules. These rules should include whether children can use virtual worlds and how they can use them.
	4.	Set mobile rules	As soon as children begin to use mobile phones, establish a list of agreed rules. These rules should include whether your children can access virtual worlds by phone and how they can use them.
Parents' education	5.	Parents should become familiar with the virtual world site (i.e. services and products offered by virtual worlds sites) and have a good understanding of how children spend their time online	Evaluate the site that children plan to use and read the privacy policy, terms of use and codes of conduct (often called "House Rules") carefully, together with any dedicated parents' page. Also, find out if the site monitors content posted on the services pages and review your child's page periodically. Check if products are sold on the site.
	6.	Activate a child's account with parent email account	The email address used to activate a child's account should always belong to a parent, not to the children.
Virtual world's features review	7.	Ensure parental control is implemented	Verify if the virtual world used by your children has a parental control or any other Internet filtering tool, and make sure such tools are activated.
	8.	Ensure parental consent is implemented	Be aware that parental consent should be required to process sensitive personal data, access chat room, send unsolicited commercial e-mails and similar, communicate with children via mobile phone, collect data from the children via the web, use children's data for any direct marketing. Exercise options carefully.
	9.	Control use of credit cards and other payment	Control the use of using landlines or mobile phones to purchase virtual items. The temptation can be too

	#	Recommendations	Description
Virtual world's features review		mechanisms	great when children are allowed to use landlines or cell phones to buy virtual items. Also, keep your credit cards under lock and key. All too often the temptation is too great to use it "just this once" without asking.
	10.	Ensure age verification is implemented	Usually age is verified when purchase of merchandise is possible, but there is currently system to guarantee age verification. Track your child's spending online carefully.
	11.	Check if the virtual world site uses automated moderation filters in conjunction with humans	Ensure that virtual world site moderates conversation with both automatic filters and by humans. This combination helps to reduce suspicious behaviour and innuendo filters may miss.
	12.	Ensure content lock is implemented	Content locks can prevent access to some un-moderated content on the web or via mobile phones. Content labelled '18-rated' or 'unclassified' can be locked with particular third party tools.
	13.	Ensure barring process/filtering is in place	Use tools to block access to undesirable websites.
	14.	Check contractual flexibility	Check how to delete an account – even if this will result in the forfeit of subscription fees. If the service will not allow an account to be deleted, consider not using it, or blocking access to it. Report such inability to delete to local authorities.
	15.	Look at the service scope	Analyse the content provider's policies and their compliance, look at the content and specific services provided, and be aware of technical limitations (e.g. adverts may be not identifiable as such).
	16.	Observe advertising, and report inappropriate advertising	Keep an eye on ads, and report to your local ad council ads that:: <ul style="list-style-type: none"> ✓ Mislead by over-simplifying complex matters. ✓ Encourage children to talk to strangers or go in danger. ✓ Show people, in particular children, using dangerous things or being close to dangerous things. ✓ Encourage unsafe emulation or dangerous practices. ✓ Encourage bullying. ✓ Cause moral harm and fear to children. ✓ Encourage bad dietary practice. ✓ Exploit a child's credibility.
Children's educations	17.	Educate your children	Education and media literacy is crucial. Explain guidelines and rules of the virtual world site when available. Children will adhere to the guidelines and often remind other players to do the same. Educate your children not to reply to rude messages and to avoid sex talk online. Teach them to not open any attachment or link they receive while chatting with

	#	Recommendations	Description
Children's educations			others because they might contain harmful content.
	18.	Explain to children never to arrange to meet in person someone they first met online	Children are in real danger when they meet in person strangers whom they have communicated with only online. Parents should encourage children to use these virtual world sites to communicate with their offline friends, not with people they've never met in person. People online may not be who they say they are.
	19.	Prevent children from sharing personally identifiable information	Help your children understand what information should be private. Explain that children should post only information that you – and they – are comfortable with others seeing. Remind your children that once they post information online, they cannot take it back.
	20.	Ensure children understand what it means to post photographs on a virtual world site, including by use of webcams	Explain to your children that photographs can reveal a lot of personal information. Children should not be allowed to use webcams or to upload any content without the approval of an adult, guardian or parent. Encourage your children not to post photographs of themselves or their friends with clearly identifiable details such as street signs, license plates on their cars, or the name of their school on their sweatshirts.
	21.	Warn children about expressing emotions to strangers	Children should not communicate with strangers directly online. Explain that what they write can be read by anyone with access to the same virtual worlds and that predators often seek children who express an interest in making new friends online.
Virtual worlds safe usage review	22.	Check child's page or profile	Check your child's page on a regular basis. Logon to view your child's account history; change your child's chat mode to a level you are comfortable with. Well-designed virtual worlds provide the opportunity for you to be deeply involved in your child's experience. If your child refuses to abide by the site's rules, contact the virtual world site and ask for child's pages and profile to be removed, further strengthening your message to your child of the importance of rules, and the consequences of breaking them.
	23.	Ensure children follow age limits on the site	If children are under the age recommended by the virtual world sites, do not let them use the sites. It is important to remember that parents cannot rely on the service provider to keep underage children from signing up.
	24.	Ensure children do not use full names	Have children use nicknames – not their real names or parts of them. Nicknames should be selected carefully, such that do not attract inappropriate attention. Do not allow your children to post the full names of their friends or any other information which could be used to identify them, such as the name of the street where they live, where they go to school, their telephone number, their sports clubs, etc.

	#	Recommendations	Description
Communication	25.	Communicate with your children about their experiences	Encourage your children to tell you if something they encounter on a virtual world site makes them feel uncomfortable or threatened. Remind your children to stop immediately any communication or content when they feel uncomfortable or suspicious. Be sure they understand they will not get in trouble for bringing something to your attention. In turn, you, as the parent and adult, should not overreact when your child shares their experience with you. Stay calm regardless of what they tell you, get all the facts, and then take action. Praise your child for trusting you. Ensure children can report abusers.