## CONTENTS

### CHAPTER 1: INTERNET SAFETY TIPS FOR YOUNG PEOPLE

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online safety</td>
<td>1</td>
</tr>
<tr>
<td>Practical tips for parents to help children and young people use the internet</td>
<td>3</td>
</tr>
<tr>
<td>Aussie kids ‘earliest internet users’</td>
<td>6</td>
</tr>
<tr>
<td>Parents’ guide to online safety</td>
<td>7</td>
</tr>
<tr>
<td>Internet safety</td>
<td>11</td>
</tr>
<tr>
<td>Offensive or illegal content</td>
<td>14</td>
</tr>
<tr>
<td>Online grooming</td>
<td>16</td>
</tr>
<tr>
<td>Top 10 tips for protecting your reputation online</td>
<td>17</td>
</tr>
<tr>
<td>Protecting personal information</td>
<td>19</td>
</tr>
<tr>
<td>Secure your mobile phone and devices</td>
<td>22</td>
</tr>
<tr>
<td>Sexting</td>
<td>25</td>
</tr>
<tr>
<td>How to help kids who are hooked on online gaming</td>
<td>27</td>
</tr>
<tr>
<td>Online gambling. So easy to bet. Too easy to lose</td>
<td>29</td>
</tr>
<tr>
<td>Online content regulation</td>
<td>31</td>
</tr>
<tr>
<td>Online content complaints</td>
<td>32</td>
</tr>
</tbody>
</table>

### CHAPTER 2: DEALING WITH CYBERBULLYING

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhancing online safety for children</td>
<td>33</td>
</tr>
<tr>
<td>Cyberbullying incidents involving Australian minors</td>
<td>36</td>
</tr>
<tr>
<td>Prevalence of cyberbullying involving Australian minors</td>
<td>37</td>
</tr>
<tr>
<td>Cyberbullying</td>
<td>38</td>
</tr>
<tr>
<td>What the experts say about cyberbullying</td>
<td>39</td>
</tr>
<tr>
<td>Cyberbullying and young people</td>
<td>41</td>
</tr>
<tr>
<td>How can we protect young people from cyberbullying?</td>
<td>44</td>
</tr>
<tr>
<td>Can a cyberbullying commissioner protect our kids?</td>
<td>45</td>
</tr>
<tr>
<td>Cyberbullying: industry against proposals to regulate social media networks</td>
<td>47</td>
</tr>
<tr>
<td>Trolling and flaming: putting out the fire</td>
<td>48</td>
</tr>
<tr>
<td>Stop the trolls: how to prevent cyberstalking happening to you</td>
<td>49</td>
</tr>
<tr>
<td>Personality differences: trolls and cyberstalkers aren’t the same</td>
<td>51</td>
</tr>
</tbody>
</table>

- **Exploring issues – worksheets and activities** | 53   |
- **Fast facts**                                    | 57   |
- **Glossary**                                      | 58   |
- **Web links**                                     | 59   |
- **Index**                                         | 60   |
Online Safety is Volume 381 in the ‘Issues in Society’ series of educational resource books. The aim of this series is to offer current, diverse information about important issues in our world, from an Australian perspective.

KEY ISSUES IN THIS TOPIC
Australians are increasingly connecting online through computers, mobile phones and other electronic devices to access the internet and social media. In the process, young people in particular are becoming more at risk of being exposed to fraud, identity theft, unauthorised access to personal information, stalking, harassment and exposure to illicit or offensive materials.

This book presents a range of cybersafety tips to arm readers with an informed awareness of the risks online and offer advice on how to stay protected. A chapter in the book is specifically dedicated to understanding and dealing with the disturbing proliferation in cyberbullying.

What are the practical ways in which we can safely communicate, access secure information and maintain healthy relationships online?

SOURCES OF INFORMATION
Titles in the ‘Issues in Society’ series are individual resource books which provide an overview on a specific subject comprised of facts and opinions.

The information in this resource book is not from any single author, publication or organisation. The unique value of the ‘Issues in Society’ series lies in its diversity of content and perspectives.

The content comes from a wide variety of sources and includes:
- Newspaper reports and opinion pieces
- Website fact sheets
- Magazine and journal articles
- Statistics and surveys
- Government reports
- Literature from special interest groups

CRITICAL EVALUATION
As the information reproduced in this book is from a number of different sources, readers should always be aware of the origin of the text and whether or not the source is likely to be expressing a particular bias or agenda.

It is hoped that, as you read about the many aspects of the issues explored in this book, you will critically evaluate the information presented. In some cases, it is important that you decide whether you are being presented with facts or opinions. Does the writer give a biased or an unbiased report? If an opinion is being expressed, do you agree with the writer?

EXPLORING ISSUES
The ‘Exploring issues’ section at the back of this book features a range of ready-to-use worksheets relating to the articles and issues raised in this book. The activities and exercises in these worksheets are suitable for use by students at middle secondary school level and beyond.

FURTHER RESEARCH
This title offers a useful starting point for those who need convenient access to information about the issues involved. However, it is only a starting point. The ‘Web links’ section at the back of this book contains a list of useful websites which you can access for more reading on the topic.
CHAPTER 1

Internet safety tips for young people

ONLINE SAFETY

The purpose of this paper from the Australian Institute of Family Studies is to provide information about online safety and relevant resources available for parents.

WHAT IS ONLINE SAFETY, AND WHY IS IT IMPORTANT?

Young people are increasingly exposed to an open and collaborative online culture, which allows them to access information, maintain friendships and relationships with family, and engage in creative content production (Collin, Rahilly, Richardson, & Third, 2011). Young people, however, are at a dynamic stage of development in which risk-taking behaviours and immature decision-making capacities can lead to negative outcomes (Viner, 2005).

An awareness of how to ensure safe practices online is an important skill for young people. While parental involvement in safe use of technology should start from a child’s first use, parents continue to be a critical influence in ensuring that teenagers practice responsible digital citizenship and engage in online activities safely.

‘Online safety’ is used interchangeably with terms such as ‘internet safety’, ‘cybersafety’, ‘internet security’, ‘online security’ and ‘cyber security’. The risk of using computers, mobile phones and other electronic devices to access the internet or other social media is that breaches of privacy may lead to fraud, identity theft and unauthorised access to personal information. Other risks for children include cyberbullying, stalking, or exposure to illicit materials. Criminal offenders have proven to be highly skilled at exploiting new modes of communication to gain access to children, and children can easily access adults-only materials if there are no protective mechanisms in place (Australian Communications and Media Authority, n.d.; Queensland Police, 2013).

These situations can place a young person’s emotional wellbeing, and in extreme cases physical wellbeing, at risk. This is particularly so where little or no attention has been paid to monitoring use, communicating with teenagers about use, or the security of the device being used. In these types of cases, and for the purpose of this paper, online safety is a child protection issue.

While online safety is important for protecting children from dangerous and inappropriate websites and materials, this does not mean that parents should discourage their children from accessing the internet. The challenge is to help children enjoy the benefits of going online while avoiding the risks (Raising Children Network, 2011).

GOVERNMENT REGULATORY PRACTICES IN AUSTRALIA

The Australian Communications and Media Authority (ACMA) works with consumers and other stakeholders in the communications industry to achieve active self-regulation and co-regulation. Together, they act to ensure compliance with license conditions, codes and standards, and the collection of both federal and state laws that apply to internet content in Australia (ACMA, n.d.).

The principle of ‘co-regulation’ reflects parliament’s intention that government, industry and the community all play a role in managing internet safety issues in Australia. ACMA also monitors the effect of regulations to ensure they are responsive to the community’s needs (ACMA, n.d.; Internet Industry Association [IIA], 2014).

MEDIA CAMPAIGNS RELATED TO ONLINE SAFETY

A number of education and awareness campaigns promoting online safety target both children and parents, yet evidence to show the effectiveness of these
Online Safety

Online Safety Issues in Society | Volume 381

campaigns remains limited (Connolly, Maurushat, Vaile, & van Dijk, 2011). Similarly, while there is evidence that cyberbullying and cybersafety programs increase young people’s awareness, there is limited evidence to show that they lead to behaviour changes (Mishna, Cook, Saini, Wu, & McFadden, 2009).

What is known is that campaigns are most effective when they integrate information with training and skill acquisition. Websites, leaflets and other information-only resources may have a limited impact when delivered in isolation. Information provided through interactive training programs, online quizzes, video games and formal curriculum assessment are more likely to translate to more secure conduct online (Connolly, Maurushat, Vaile, & van Dijk, 2011). For this reason, parents are encouraged to facilitate their children’s engagement with age-appropriate interactive learning materials related to online safety.

The following is a snapshot of campaigns that provide targeted and interactive online learning opportunities for children and parents.

**BackMeUp – Australian Human Rights Commission**
BackMeUp is a campaign that includes a video competition in which teenagers have the opportunity to take a stand against cyberbullying.

**Bravehearts online**
Internet safety resources focus on online risks; information for young people; information for parents and carers; internet safety contacts and further links and resources.

**Make cyberspace a better place – KIDS Helpline**
Kids Helpline campaigns to help children enjoy the freedom and fun of using the internet and to and help make cyberspace a fun and safe place.

**Smart online, safe offline (SOSO) – National Association for Prevention of Child Abuse and Neglect (NAPCAN)**
By using social networking environments to target children and young people directly, the SOSO initiative educates children and young people about the dangers that exist online and on how they can manage their personal safety.

**Tagged (Cybersmart) – ACMA**
Developed by the ACMA’s Cybersmart program, Tagged has received acclaim for its realistic depiction of teenagers and the problems they can face in a digital world. Since its launch in September 2011, Tagged has become a popular resource for Australian teachers and parents. More than 10,000 copies of the film and posters have been distributed nationwide and it has attracted nearly 50,000 views on YouTube.

**The Alannah & Madeline Foundation – Keeping children safe from violence**
This national charity aims to protect children from violence and its devastating impact. The website provides a range of information and resources for parents and children, including an evidence-based educational program (eSmart Schools), and a variety of other resources about bullying and cybersafety.

Some campaigns are delivered in collaboration with a wide variety of public and private agencies. As a result, there is a large degree of crossover in the material of various contributors presented across the websites. Furthermore, initiatives may target a specific issue (such as cyberbullying), or they may be delivered as part of a broader social awareness campaign (child protection). For additional resources about online safety, see ‘Further Resources’ below.

THE SIGNIFICANCE OF 13 YEARS OLD
As part of their privacy policies, social networking sites such as Facebook, Twitter and YouTube specify that users must be at least 13 years old, a requirement of which parents may often be unaware.

The minimum age stipulations are based on the requirements of the US Congress as set out in the Children’s Online Privacy Protection Act. The Act specifies that website operators must gain verifiable parental consent from parents prior to collecting any personal information from a child younger than 13 years old (O’Keeffe et al., 2011). As such, many social networking sites avoid this requirement by setting a minimum age of use at 13 years old – but there is no onus on website operators to verify the age of users.

FURTHER RESOURCES
Online safety information is easily accessible through any search engine, and numerous sites are devoted specifically to this issue. This section identifies several Australian websites about online safety that can be useful for parents and caregivers.

**Cybersafety help button download page**
The Help Button provides internet users, particularly young people, with a ‘one stop shop’ for cybersafety

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: St Mark’s Anglican Community School, Hillarys, libraryadmin@stmarks.wa.edu.au
Practical tips for parents to help children and young people use the internet

The following tips will help parents provide support and guidance for children and young people as they increasingly engage in online activities.

**Monitoring and supervision**

Monitoring a young person’s online activities includes checking that websites are appropriate for a child’s use and keeping an eye on the screen, with parental checks more likely to occur at younger ages. If parents are willing to provide children and young people with access to mobile phones and computers, then a responsibility to understand, role model and communicate the basics of good digital citizenship should come with the access.

Advice on monitoring often focuses on keeping the computer in a shared family area, yet in the age of wireless connections and internet-enabled smartphones, this is increasingly difficult. Similarly, young people may control their own online details, such as passwords and hiding web browser histories.

Ways in which these difficulties can be addressed include:

- Developing a plan about internet use in partnership with family members. This can include:
  - Details of appropriate online topics
  - Privacy setting checks
  - Limits on screen time
  - Limits on when wireless internet connections and/or mobile devices will be available, and
  - What may be identified as ‘inappropriate posts’ on online profiles.
- An ‘internet use agreement’ may be useful to develop with older children.
- Taking an active role in discussing the benefits of online activities with children and young people, and what strategies they may use to respond to cyberbullying, other negative online behaviours, or if they unintentionally access adult content. Discussions can include how these rules may apply wherever they are online, including at home in their bedroom and when they are outside the home, for example, at a friend’s place.

**Protection**

Parents can be encouraged to:

- Find out whether their child’s school has an internet policy and how online safety is maintained. Inquiries should focus on the strategies used to educate children and young people about online safety and cyberbullying, whether parents are involved in cyberbullying initiatives and if they are involved in developing cyberbullying policies.
- Point out to children that some websites on the internet are for grown-ups only and are not intended for children to see. Discuss what strategies a teenager might adopt if he/she accesses this content.
- Use a family-friendly internet service provider (ISP) that provides proven online safety protocols. Filtering tools should not be solely relied on as a solution, however – open discussion and communication with young people about monitoring and supervision is needed.
- Empower children to use the internet safely by mutually exploring safe sites and explaining why they are safe. It’s also important to educate children on why it’s not safe to give out any personal details online.

**Engagement and communication**

Parents can be encouraged to:

- Discuss with children how they may recognise the difference between online information that is helpful or unhelpful, true or false, useful or not useful. For example, government or education websites may contain more accurate information than opinions that are posted on an unfamiliar person’s blog.
- Increase their own knowledge and become more adept at engaging in online activities and exploring social networking sites that are being used by their children. Learning alongside children and young people can be an effective way to achieve this – parents can be encouraged to let their children be the ‘experts’ and help them understand the tools they are using online.
- Focus on the positive aspects of the internet – spend time looking together at sites that are fun, interesting or educational. Find sites together than are age- and stage-appropriate for children.
- Encourage your child to question things on the internet. When looking at a new site, your child could ask questions such as, “Who is in charge of this site?” , “Have I found information, or is it just opinion?” or “Is this site trying to influence me or sell me something?”.

**Report**

If you have found any material online that you believe is prohibited or inappropriate, you should contact the ACMA. For further information, go to the ACMA’s website [www.acma.gov.au](http://www.acma.gov.au), where a range of resources are available for parents and caregivers.

information and assistance. Once downloaded, the button sits on the desktop or in the tool bar. When double clicked, the button allows users to talk, report or learn about cybersafety issues such as cyberbullying, scams and fraud, and unwanted contact.

**Australian Council on Children and the Media (ACCM) – Promoting healthy choices and stronger voices in children’s media**

This is a source of up-to-date information about media and children, for parents and caregivers, professionals, students and researchers. The information is drawn from worldwide research studies, current literature, surveys, statistics and other authenticated sources of information. Contact numbers and helplines are provided to report breaches of internet security or to access advice about appropriate action to take.

**Australian Government Resources Hub**

This resource from the Australian Government provides a range of links to key sites and agencies that are devoted to internet safety.

**Budd:e – Stay smart online**

Budd:e is an award winning cyber security education package with fun and challenging interactive games that help Australian students stay safe and secure online. The package includes self-learning modules for primary and secondary students as well as with resources for teachers and parents.

**Cybercrime – Australian Federal Police (AFP)**

Child protection operations of the AFP are responsible for the investigation of crimes associated with online child sex exploitation and child sex tourism. The links provided allow access to a wide range of helpful materials and resources, including the AFP’s website, where the ‘top ten tips for youth’ on cybersafety can be found.

**Cybersafety help and advice – Department of Communications**

The Department of Communications provides a hub of information about cybersafety in a simple format, with information about where and how to report risky online behaviour, and how to stay safe online. The site also provides an easy guide to socialising online.

**Cybersmart – ACMA**

Cybersmart provides activities, resources and practical advice to help young kids, kids, and teens safely enjoy the online world. The links contain audio-visual materials, tips and links plus additional resources for school teachers. A catalogue of useful library resources is also provided.

**Cybersmart Parents – ACMA**

This resource is designed to assist parents to help their children enjoy safe and positive experiences online. It provides information on how children and young people use the internet, contains various strategies to manage risks and describes the issues children face in the online world.

**Images of Children and Young People Online (NCPC Resource Sheet)**

This Resource Sheet contains information about legal issues, privacy laws, emerging issues, classifications of online images, good practices, lodging a complaint about a website and links to additional resources.

**Internet Industry Association (IIA) – Guide for internet users**

This guide assists Australian internet users to understand Australia’s co-regulatory framework for online content, pursuant to the requirements of legislation. The IIA is a non-profit, private sector industry body that, among other things, develops best practice rules for the industry in Australia in conjunction with ACMA.

**Learning On Line – Victorian Department of Education and Early Childhood Development**

The Learning On Line website provides advice for schools on cybersafety and the responsible use of digital technologies. It has been developed to help schools make the most of the opportunities presented by new developments in digital technologies.

**Parental Involvement in Preventing and Responding to Cyberbullying (CFCA Paper)**

This paper from the Child Family Community
Australia information exchange outlines definitions and statistics related to cyberbullying. It explores the differences between cyberbullying and offline bullying, and parents’ roles and involvement in preventing and responding to cyberbullying incidents. The aim is to inform practitioners and professionals of ways to help parents clarify their roles, and provide them with the tools to help their teenaged children engage in responsible online behaviour.

Raising Children Network – Safety tips for parents of toddlers to teens (ages 4-15)

The Raising Children Network website displays tabs for each phase of a child’s development, from newborns to early teenagers. Internet safety tips and a comprehensive range of resources are provided to cater for each specific age group, with the exception of newborns and toddlers.

Schoolatoz – NSW Department of Education and Communities

Practical help for parents about cybersafety and keeping kids safe online are provided in the schoolatoz website. It includes ten cybersafety tips every parent should know, and information from experts about the issue. Useful information is also provided for parents of children who are bullied.

Stay Smart Online

This is a one-stop shop providing information for Australian internet users on the simple steps they can take to protect their personal and financial information online. The site has informative videos, quizzes and a free Alert Service that provides information on the latest threats and vulnerabilities.

ThinkUKnow – Internet safety program

ThinkUKnow is an internet safety program delivering interactive training to parents, carers and teachers. Created by the UK Child Exploitation and Online Protection (CEOP) Centre, ThinkUKnow Australia has been developed by the Australian Federal Police (AFP) and Microsoft Australia. Users will need to subscribe to the site to gain access to its tools and resources.

Who’s chatting to your kids? – Queensland Police resource

A brochure published by the Queensland Police Service’s Task Force Argos. This brochure provides information to parents on internet safety for children and young people. It discusses social networking, mobile phones, webcams and online gaming, and provides information about the types of things to look out for that may indicate that children could be at risk.

Some of the more popular social networking sites provide information specifically tailored to help parents understand their child’s use of the site. For example:

- Facebook: Help your teens stay safe
- YouTube: Parent resources

References


This paper was updated by Rose Babic, Project Officer, and Elly Robinson, Manager, Child Family Community Australia information exchange, Australian Institute of Family Studies.

Endnotes

1. For access to codes relating to internet use, see ‘Initiatives and codes’ on the Internet Industry Association (IIA) website.
2. Further information: How to comply with Children’s Online Privacy Protection Act.

Commonwealth of Australia 2014.
Aussie kids ‘earliest internet users’

Australian children are among the youngest and prolific users of the internet in the world, according to a new study from the ARC Centre of Excellence for Creative Industries and Innovation that compared the experience of Australian children aged 9-16 to those of their European counterparts.

The study, AU Kids Online, was authored by Professor Lelia Green, Professor John Hartley and Professor Catharine Lumby from the ARC Centre of Excellence for Creative Industries and Innovation (CCI). It was carried out in parallel with a 25-nation survey in the Europe.

Four hundred 9-16 year olds and their parents or carers were interviewed face to face for the study. “This is the first Australian study of its kind where children were directly interviewed on a large scale about their online experience,” says Prof. Green. “It gives us significant empirically sound information about the opportunities and the risks for Australian children in the online and mobile media era.”

A key finding of the study is that Australian children were on average a little under 8 years old when they began using the internet – making them among the youngest users in the 26-nation study.

The study reports that 76 per cent of Australian children and young teenagers go online daily, with the average time spent online bordering over one and a half hours per day.

“One of the pleasing findings was that parental mediation of online use and safety was high in Australia and that teachers were also very active in guiding children on internet use,” said Prof. Green.

“However, 30 per cent of Australian children reported encountering something online that upset or bothered them – two and a half times the European average. The content predominantly related to online bullying and sexual images, which were more likely to bother younger users.”

Professor Green said this finding pointed to the need for further focus on supporting parents, teachers and carers to give children and teenagers tools to manage their online experience.

“The study reveals that while a minority of children are upset by online risks, many benefit from the advice and tools available to them. The risks and opportunities of the online world go hand in hand for children and it is important to avoid being overly restrictive.”

Professor Lumby noted that the study showed that Australian children and teenagers were not only using the internet to passively consume material – they were actively creating and sharing content, with almost half photos, videos or music.

She added: “This study shows that now is the time for Australia to invest in supporting educational initiatives to keep our children safe online and able to explore the significant benefits of online learning and social networking.”


It draws on the work of the EU Kids Online network funded by the EC (DG Information Society) Safer Internet plus Programme (project code SIP-KEP-321803); see [www.eukidsonline.net](http://www.eukidsonline.net)

The ARC Centre for Excellence for Creative Industries and Innovation (CCI) is helping to build a creative Australia through cutting edge research spanning the creative industries, media and communications, arts, cultural studies, law, information technology, education and business. It is funded by the Australian Research Council (ARC).

PARENTS’ GUIDE TO ONLINE SAFETY

Practical, issue-focused information and advice for parents of children of all ages, from the Australian Communications and Media Authority

Cybersmart is a national cybersafety education program managed by the Australian Communications and Media Authority (ACMA) as part of the Australian Government’s commitment to cybersafety. The program is specifically designed to meet the needs of children, young people, parents and teachers.

CYBERBULLYING

Cyberbullying is the use of technology to bully a person or group. Bullying is repeated behaviour with the intent to harm others.

Behaviour may include:
- Abusive texts and emails
- Posting unkind or threatening messages, videos or images on social media websites
- Imitating or excluding others online
- Inappropriate image tagging.

For many teenagers, their online life is an important part of their social identity. Many young people fear that parents might take away their devices and refuse access to the internet and so do not report cyberbullying to their parents. Teenagers are also often concerned that parents’ actions will make cyberbullying issues worse, so it is important to remain calm and supportive.

Trolling is when a user intentionally causes distress by posting inflammatory comments online.

Trolling differs from cyberbullying in that trolls aim to gain attention and power through disruption of conversation by encouraging a defensive reaction from those they attack. Cyberbullying usually focuses less on the reaction of the victim, and more on the feelings and authority of the bully. Cyberbullying is usually repeated behaviour, while trolling can be one-off.

What can I do?

As a parent, you can help your child and encourage them to take control of the issue.
- Talk to them about cyberbullying before it happens. Work out strategies to address any potential issues and reassure your child that you will be there to support them.
- Advise your child not to reply to any messages from a bully. Often if bullies don’t receive a response they will give up.
- Learn how to block a bully so they are no longer able to make contact.
- Keep a record of harassing messages in case authorities become involved. Put them somewhere your child won’t continue to see them.
- Contact the website administrator or use the reporting function to ask for content to be removed or to report harassment.
- Talk to your child’s school if cyberbullying involves another student. The school should have a policy in place to help manage the issue.
- Remember that if your child has been involved in cyberbullying and seems distressed or shows changes in behaviour or mood it may be advisable to seek professional support, including through the Cybersmart Online Helpline at cybersmart.gov.au/report.aspx

SOCIAL NETWORKING

Social networking describes a variety of services like Facebook, YouTube, Instagram, World of Warcraft, Moshi Monsters, Twitter, Skype, Snapchat, Minecraft and many others.

All of these services enable direct interaction between individuals. Users can post information about themselves, display photos, tell people what they’ve been up to, chat and play games. Social networking forms a part of the social identity of many teenagers.

Grooming

Online grooming is the illegal act of adults making contact with a child online for the purpose of establishing a sexual relationship. Often this will be via a social networking site, but it may also be through other online services.

What can I do?

As a parent, you can help your child have positive experiences on social networking sites.
Stay involved in your child’s use of new technology. Set up your own account and learn about privacy settings so you can understand how you can best protect your child. It can be fun for you too!

Check the age restrictions for the social networking service or game. Some social networking sites (such as Club Penguin) are created especially for children under the age of 13, but most mainstream sites like Facebook, Instagram and others require the user to be 13 or older.

Advise children to set their accounts to private so that only people they want to see it can view their information.

Encourage children to think before they put anything online. Information posted online can be difficult or impossible to remove. An inappropriate image posted today can have a long-term impact on their digital reputation.

Show them how to set up location services on their phone so they are not inadvertently broadcasting their location.

Remind children to be careful when making new friends online; people may not be who they say they are. Never arrange to meet an online friend unless a trusted adult is with them.

Report any abuse or inappropriate content to the social networking site and show children how to do this too.

Learn how to keep a copy of online conversations and how to block people prior to an issue occurring.

For more information on managing your children’s access to particular social networking sites, visit cybersmart.gov.au/parents.aspx

SEXTING

Sexting is the sending of provocative or sexual photos, messages, or videos, generally using a mobile phone or webcam. It can also include posting this type of material online. Young people often consider sexting as a way of connecting in a relationship.

What can I do?

• Talk to your child about sexting to prevent any issues from arising. Make sure they are well aware of the risks that may occur if their images were to be spread beyond the person they intended them for.

• Remind your child about the social and legal consequences of sexting. If anyone in the photo or video is under 18 they may be committing a crime if they send, receive or forward messages.

• If your child has been involved in sexting, remember to stay calm and be reasonable about the consequences. Sexting is not uncommon behaviour and your child is not alone in being negatively impacted. Rather than adding to the distress, focus on finding a solution for your child.

• Try to get the image/video removed from all locations to the greatest extent possible. If sexting content is posted online, report it to the website administrator.

• Seek help from the school if necessary. Ask them to help track who might have the image or video and where it might be posted. Ask them to provide support to your child and others involved.

• Ensure that your child is supported if they have been negatively impacted by sexting. Their friends are critical so try to help them stay connected to them for support, both online and offline.

MOBILE PHONE SAFETY

Mobile phones are a great way for children and teenagers to stay in touch with their parents, family and friends and provide access to fun and functional resources like games, the internet, music, apps and more from anywhere at any time.

Many young people would never be without their mobile phone, and a mobile phone provides you with immediate access to your children. However, the fact that they are 24/7 and you can’t always be there to supervise means there are potential risks. These can include high or unexpected bill costs, cyberbullying, sexting, broadcasting their location to unintended others through ‘checking in’ and access to inappropriate material.

What can I do?

• If you think your child needs a mobile phone, consider purchasing a phone that is not internet-enabled.
Smartphones come with features you may not yet want your child to have such as unsupervised internet access, a camera, and a wide variety of online games and apps.

- Stay involved with your child’s use of their mobile phone. If you don’t have a good understanding of how their phone works and what they use it for, ask them to show you.
- Help your child to understand that they should treat their phone like a wallet, and that every text message, phone call or download costs money.
- Let your child know that it’s OK to tell you if they come across something that worries them, and that their phone won’t be taken off them if they report something to you.
- Investigate phone plans and pre-paid contracts. Decide what your child needs from their mobile phone so you are well-educated on options before you approach a provider.
- Check automatic download settings and in-app purchase settings on your child’s mobile phone, as these can incur extra costs or use up credit quickly.
- Consider keeping credit card details away from your children so music and apps cannot be purchased without your knowledge. If you have your credit card details stored on an online account, you may choose to keep the password to this account private.

**OFFENSIVE OR ILLEGAL CONTENT**

Children and young people may not deliberately seek out inappropriate content. Children can inadvertently access disturbing or illegal content while undertaking online searches or by clicking on unknown links.

Offensive or illegal content may include topics, images or other information that are prohibited in Australia or could be damaging to young people online.

This is content that may:

- Include footage of real or simulated violence, criminal activity or accidents, promote extreme political or religious views or be sexually explicit and can include illegal images of child sexual abuse.
- Promote hate towards individuals or groups on the basis of race, religion, sexual preference or other social/cultural factors, instruct or promote crime, violence or unsafe behaviour, like bomb or weapon making, anorexia, drug use, gaining unauthorised access to computers, fraud or terrorist activities.

**What can I do?**

- Be aware of how your child uses the internet and explore it with them. Discuss the kinds of sites that are ok to explore and those that are not.
- Consider using parental controls such as filters to help manage your child’s online access.
- Remind your child not to open spam email or click on pop ups, prize offers or unfamiliar hyperlinks in websites.
- Help your child use search engines to locate websites. Consider developing a list of favourites for younger children. Enable safe search options.
- Reassure your child that access to the internet will not be denied if they report seeing inappropriate content to you.
- Remind them not to respond if they are sent something inappropriate and that they should leave a website immediately if they feel uncomfortable or worried.
- Report content that you think may be prohibited to the ACMA’s online hotline: acma.gov.au/hotline

**HOW MUCH IS TOO MUCH?**

Your child may be spending too much time online if their online behaviour is having a negative impact on other aspects of their life.

To many parents it can seem as though children and young people are constantly online. Often they are multitasking; for example downloading and listening to music while studying and chatting with friends or sending messages on their mobile phones.

The number of hours children and young people spend online can vary significantly. There is no guideline for the ‘right’ amount of time for children to spend online, however if their online behaviour appears to impact...
negatively on their behaviour or wellbeing, or that of the family, it may be time to discuss expectations and establish time limits.

**What can I do?**

- The longer you wait to address the issue, the more difficult it can be to overcome. So if you see an emerging problem arising from excessive use, act on it right away.
- Talk to your child about the concerns you have and monitor what games, apps and devices are bought or used by your child.
- You may like to install a filter on the laptop or computer your child is using which can be adjusted to limit the amount of time an internet connection will be available on that device.
- Consider implementing family agreements about the amount of time your children can spend online. You might like to have a rule where the ‘wifi password of the day’ is only given once all homework/chores/family time is done. A similar approach can be used to limit access to devices.
- If your child seems particularly anxious or irritable, or you notice them seeming isolated from friends or other activities, there may be an underlying mental health issue. Consider getting help from school counsellors or your GP who can refer your child to a professional psychologist.

**HELP AND RESOURCES**

Check out the following support services and resources to help you keep your family safe online.

- The Cybersmart website contains information and related links to support parents in keeping kids safe online. Resources include practical, action-focused advice, videos, games, support, and research-based information, and everything is free of charge. Visit cybersmart.gov.au
- Cybersmart Outreach offers free, school-based presentations to keep parents, students and teachers up-to-date with cybersafety issues. These sessions are informative, non-technical and available to all schools. Ask your child’s school if they have registered to host a presentation. Visit cybersmart.gov.au/outreach.aspx
- School support – Schools may have detailed policies and procedures in place to help support children online, including how to manage issues like cyber-bullying, sexting and other online concerns. For more information, contact your child’s school.
- Counselling – If you suspect or know that a child is being negatively impacted by things happening to them online, consider seeking professional support for them including through the Cybersmart Online Helpline, provided by Kids Helpline. The service provides free, confidential online counselling for children and young people. Visit cybersmart.gov.au/report.aspx
- The Department of Communications’ *Easy Guide to Socialising Online*, provides information on the safe use of social networking sites, games and search engines. Visit communications.gov.au/easyguide

**SOCIAL**

Facebook (teenagers): facebook.com/cybersmartcloud
Facebook (parents): facebook.com/cybersmartacma
Twitter: @CybersmartACMA
YouTube: ACMACybersmart

**CONTACT US**

Email: cybersmart@acma.gov.au
Phone: 1800 880 176

Cybersmart, through Kids Helpline, also provides young people experiencing problems online with free and private web chat counselling.

Phone: 1800 55 1800

All of Cybersmart’s information, games, videos and teacher resources are available free-of-charge from cybersmart.gov.au

© Commonwealth of Australia.

Australian Communications and Media Authority.

INTERNET SAFETY

The internet can be a powerful tool for learning. It’s also a place where your child could encounter dangerous material or people. Your challenge is to help your child enjoy the benefits of the internet while avoiding the risks. A fact sheet from Raising Children Network

Benefits of the internet

Children can benefit from the internet because it offers them more text-based information than other media. This can help improve a child’s reading and problem-solving skills. Some studies show that the internet can make learning more fun for young people.

Children can also benefit socially because they use email, chat rooms, forums and social networking sites such as Facebook and MySpace to communicate with friends (although face-to-face communication is also important for social development).

Monitor

You can monitor and supervise your child’s use of the internet in several ways:

- Talk with all family members about internet access. Monitoring works best if you are able to have calm and frank discussions with your child about his internet activities.
- Keep the computer in a shared family area. If possible, avoid putting it in a study or bedroom. This allows you to keep tabs on how long your child is online as well as what websites she is visiting.
- Together with your child, set up some simple and fair rules about internet use. For example, set a reasonable limit on the amount of screen time that your child is allowed. Discuss how these rules apply outside your home – for example, at a friend’s house or the local library. When your child follows the rules, remember to give him lots of positive feedback.
- If you have older children, it’s a good idea to have a written internet use agreement with them. A written agreement signed by both of you helps make rules clear.
- Your browser program contains a History button, which will allow you to see websites that your child visits.
- Find out if your child’s school has an internet policy and how internet safety is maintained there.

Protect

You can help protect your child while she is using the internet:

- Explain to your child that not all information on the internet is good, true or helpful. Explain also that some areas are for adults only and not intended for children to see.
- You can help your child identify unsuitable material by naming some things to look out for. For example, a site containing scary or rude pictures, swearing or angry words is probably not suitable.
- You can use a family-friendly internet service provider (ISP) such as Optus or Telstra BigPond. You can also suggest safe search engines like www.awesomelibrary.org to your child and bookmark them for later use.
- Ask your child to let you know if a person he doesn’t know contacts

DID YOU KNOW?

Most child development experts recommend limiting children’s daily screen time. Screen time includes TV, DVD and computer time.

Current Australian guidelines are no more than an hour a day for children aged 2-5 years, and no more than two hours a day for children over five.
him. Also, your child should tell you if he’s planning a face-to-face meeting with someone he has met online. In this case, he should ask an adult he trusts (such as mum, dad, older brother or sister, or another adult) to go with him. The meeting should always be in a public place, preferably during the day.

Teach
You can help your child learn how to use the internet safely, responsibly and enjoyably:

• Focus on the positive aspects of the internet when you’re guiding your child. Spend time showing him sites that are fun, interesting or educational (and then bookmark them for later use). For example, you could help your child find some information he needs for homework.
• Encourage your child to question things she finds on the internet. When she finds a new site, she could ask herself questions such as, “Who is in charge of this site?”, “Have I found information or is this just opinion?” and “Is this site trying to influence me or sell me something?”
• Use an educational program specifically designed for your child’s age group.
• Empower your child to use the internet safely by showing her safe sites and teaching her why they are safe. It is also important to educate your child on why it is dangerous to give out any personal details online.

Learn
If you’re not familiar with the internet, start by learning about it yourself:

• All you need is a basic understanding to help you supervise and guide your child. You can check out community resources such as your local library, neighbourhood house, TAFE or Council of Adult Education programs. Many of these will provide classes or further information.
• Be reassured that you’re not alone if you find that your child knows more about the internet than you do. So why not ask your child for a lesson? This can be fun for both you and helps you understand just how much your child does know.

Common concerns about children’s internet use

Access to inappropriate content
Children might be only one or two clicks away from violent, pornographic or offensive material (even accidentally), especially if there are no filters or monitoring software installed on your computer. Some websites might contain advertisements for alcohol or cigarettes directed at children. These can be difficult to block, because they are...

INTERNET SAFETY TIPS

<table>
<thead>
<tr>
<th>PARENT CONCERN</th>
<th>TIPS FOR PARENTS</th>
<th>WHAT TO TELL YOUR CHILD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding unsuitable material</td>
<td>Use a screening program or filter to block entry to certain websites. Filters are not 100% effective but are worth looking into. Many ISPs offer internet filters as part of their service. Buy and install a program that will block emails or web pages containing unsuitable key words. If your child finds unsuitable material, discuss the material calmly. Let your child know how pleased you are that she is talking to you about it.</td>
<td>If you come across material that scares you or makes you feel uncomfortable, tell mum, dad or a teacher.</td>
</tr>
<tr>
<td>Giving personal information to strangers</td>
<td>Anything you put into a computer or text message could become public property.</td>
<td>It’s very important to check with mum, dad or a teacher before you give out any personal details to anyone, especially if you don’t know the person.</td>
</tr>
<tr>
<td>Rules and behaviour</td>
<td>If you have agreed on internet rules and your child breaks them, you can block your child’s access to the internet. To do this, remove the modem and attach it only when you can supervise.</td>
<td>Remember how we agreed on the rules and why we have them.</td>
</tr>
</tbody>
</table>
also some chat rooms can encourage inappropriate or harmful behaviour such as extreme dieting, underage sex or drug use.

**Filter programs**
Filtering programs are not completely effective. A resourceful child can sometimes find ways to get around these programs. Filters don’t screen what goes on in chat rooms. They can’t replace parental awareness and supervision.

Also, recent research tells us that ‘server-based’ filter programs (the kind your internet provider might run) are generally difficult to maintain. Their performance depends a lot on how they’re set up and fine-tuned. It’s worth checking the features of such programs carefully. You might need to add on extra features or programs.

**Paedophilia**
Chat rooms and forums are lots of fun and great places to exchange ideas, but they can be risky. They allow people to interact anonymously, and age limits can’t be enforced. Also, children might be invited to meet up in the real world with people they meet online, which could lead to sexual or physical abuse.

The risk of stalking or child abuse over the internet can be avoided if you advise your children never to give personal information to or communicate one to one with people they do not know. Paedophiles have fewer opportunities to target children if personal information is not revealed.

**Leaking of personal information**
This is more of an issue for older children. It can occur by accident when children provide personal details on websites or to strangers they have met online. Risks include cyberbullying or identity fraud.

**File-sharing programs**
Online software that enables files to be swapped over the internet is a very attractive way for kids to share MP3 songs, videos and images for free. But sharing music and other files over the internet is against the law. Legal action has been brought against people for doing it.

These kinds of file-sharing programs, often called ‘peer-to-peer’ programs, also allow access to your computer by strangers who could introduce computer viruses or other harmful material.

**Too much internet/computer use**
Parents sometimes worry about their children using the internet too much. If a child is already shy or uncomfortable in social situations, that child might spend a lot of time online, withdrawing from family and friends. If most or all of a child’s interaction with friends is via computer – instant messaging, emails, chat rooms – this can affect the development of the child’s social skills.

**INTERNET FACTS AND STATS**

- More than 50% of Australians have the internet at home. Also, a household with children is more likely to have a computer with internet access.
- Boys and girls use the internet an equal amount, but there are some differences in how they use it. Research has shown that boys play more online games than girls, and girls use chat rooms and education sites more than boys do.

**GLOSSARY**

**Chat room**
A site on the internet where people communicate by sending messages to each other. When someone types a message on their computer, it appears on the screen in real time and other people can read it. Online chat is not usually stored permanently on the internet.

**Forum**
A place on the internet where people can discuss topics of interest by submitting a message. Unlike some other online discussion spaces, such as chat rooms, forums do not necessarily work in real time. Forums are often presented as part of websites. Forum discussion is usually stored and can be accessed indefinitely. Forums are often reviewed by an administrator.

**Facebook**
A website that allows users to build an online profile with personal details, photos, videos and other information. Users can add friends, send them messages, and let friends know what they are doing via ‘status updates’. Users can also comment on their friends’ status updates, photos and videos. These activities are called social networking.

**MySpace**
A website that allows users to create an online profile with information about themselves, their interests and their moods. Users can upload music, photos, videos and blogs. They can receive comments from other users. MySpace has a group feature, which allows users with common interests to share a page. Activities like these are called social networking.

**Filter**
A piece of computer software that monitors and restricts access to internet content.

**Privacy**
This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: St Mark’s Anglican Community School, Hillarys, libraryadmin@stmarks.wa.edu.au

Children and young people may not deliberately seek out inappropriate content. Children may inadvertently access content while undertaking online searches or they may seek it out or be referred content by others. Young people with smartphones might discover content that may be blocked by home and school internet filters.

Inappropriate content can expose children to concepts that they are not ready to manage and that may breach social and cultural norms. Some content can be distressing for children. They may not report it to parents or teachers as they may be ashamed of what they have seen, particularly if they sought it out.

This is content that:
• Includes footage of real or simulated violence, criminal activity or accidents, from video clips, games or films
• Is sexually explicit and can include illegal images of child sexual abuse
• Promotes extreme political views, potentially used in the radicalisation of vulnerable members of the community
• Promotes hate towards individuals or groups, on the basis of race, religion, sexual preference or other social/cultural factors
• Instructs or promotes crime, violence or unsafe behaviour, like bomb or weapon making, drug use, gaining unauthorised access to computers, fraud or terrorist activities
• Online advertising which promotes adult content.

Some content that is considered inappropriate may also be prohibited or illegal in Australia. Prohibited content is defined with reference to the National Classification Code categories RC, X18+, R18+ and MA15+. While it is not an offence to view or possess prohibited content, the ACMA can take action under the Broadcasting Services Act 1992 to restrict the availability of such material. Further information on prohibited online content, including how to make a complaint to the ACMA if you or a student comes across this type of content, is available on the ACMA’s website, www.acma.gov.au

HOW DO CHILDREN ACCESS INAPPROPRIATE CONTENT?

Children may be exposed to such content through otherwise innocuous activities, such as:
• Unexpected results from online searches
• Clicking on unknown links within websites or emails
• Incorrectly typing a web address or clicking on a pop-up ad
• Clicking on online game content or prize offers.

In some cases children and young people deliberately access inappropriate material, particularly as they move into adolescence. This can be out of curiosity or to share with peers for the ‘shock value’ of the content.

Inappropriate content can expose children to concepts that they are not ready to manage and that may breach social and cultural norms. Some content can be distressing for children. They may not report it to parents or teachers as they may be ashamed of what they have seen, particularly if they sought it out.
WHAT IS PROHIBITED ONLINE CONTENT?

Some content that is considered inappropriate may also be prohibited or illegal in Australia. Prohibited content is defined with reference to the National Classification Code categories RC, X18+, R18+ and MA15+.

While it is not an offence to view or possess prohibited content, the ACMA can take action under the Broadcasting Services Act 1992 to restrict the availability of this type of material. Content that is prohibited is any online content that is classified RC (refused classification) or X18+ by the Classification Board.

Further information on prohibited online content, including what constitutes prohibited content and how to make a complaint to the ACMA if you or your child comes across this type of content, is available on the ACMA’s website, www.acma.gov.au

LIMITING CHILDREN’S EXPOSURE TO INAPPROPRIATE CONTENT

Filters, labels and safe zones enable parents to reduce children’s risk of exposure to unsuitable or illegal sites and to set time limits for internet access. When deciding which tools are the most appropriate for your family, it may be useful to consider the level of guidance needed from you and balance this against your children’s ages and the range of content they may need to access.

PC filters

PC filters are computer software programs on your computer which offer a range of different functions to block, screen or monitor inappropriate content. Many filters can also be customised to suit the internet activities of each user.

Common features of PC filters include:
• Category blocking which enables the user to select from a range of content categories. For example pornography and violence, and decide which to block and which to allow
• Time controls, which allow users to limit internet access to certain times of the day, including the amount of time a child spends on the internet. This can help ensure children can only use the internet when parents are available to supervise and can restrict late night use which is tempting for some teens
• Logging which enables parents to track and record a history of sites visited by their child
• Service blocking which allows users to block or filter access to certain services, such as peer-to-peer, social networking or online games.

The ACMA regularly updates a list of prohibited content. These web pages are blocked by the internet content filters listed under the Internet Industry Association Family Friendly Filters program.

Filters, labels and safe zones enable parents to reduce children’s risk of exposure to unsuitable or illegal sites and to set time limits for internet access. When deciding which tools are the most appropriate for your family, it may be useful to consider the level of guidance needed from you and balance this against your children’s ages and the range of content they may need to access.

Server level filters

Server level filters are able to block internet content before it reaches the home. These filters are most commonly provided by internet service providers (ISPs).

Internet filters are no substitute for parental guidance and supervision. No filtering tool can block all unsuitable material. As the internet is vast and constantly changing, lists of blocked sites must be continuously updated for the filter to work effectively. Even then, some undesirable sites may still slip through the filter.

Labels

Labelling tools attach descriptive tags to websites. Most browsers can read these labels and be programmed to block access to these sites or advise when sites are unsuitable for children. Labelling tools can also complement filtering tools.

Websites can be labelled according to how suitable they are for children or to identify the sort of material that they contain, for example, medium-level sexual activity. These tools, together with a web browser, enable
users to set levels of access for labelled sites, blocking access to anything above those levels. Some browsers also allow users to restrict access to unlabelled sites.

While labelling tools are useful, most websites are still unlabelled.

**Safe zones**

Safe zones are secure networks offering access to a range of sites specially designed for children and therefore with little risk of exposure to inappropriate content. Many safe zones are free of charge but some are subscription based, requiring a special login and password as they are protected from other areas on the internet.

**WHERE DO I GO FOR HELP?**

**Reporting inappropriate or illegal content**

Further information on prohibited online content, including what constitutes prohibited content and how to make a complaint to the ACMA if you or your child comes across this type of content, is available on the ACMA’s website, www.acma.gov.au

**Counselling**

**Kids Helpline**

Kids Helpline provides free, confidential online and phone counselling for 5-25 year olds.
Ph: 1800 55 1800
Web: kidshelpline.com.au

**eheadspace**

eheadspace is for 12-25 year olds in need of support or worried about their mental health.
Ph: 1800 650 890
Web: eheadspace.org.au

**Cybersmart Outreach internet safety awareness presentations**

Cybersmart Outreach offers free Internet Safety Awareness presentations for parents, students and teachers. These sessions are informative, non-technical and available to all schools. Ask your child’s school if they have registered to host a parent presentation.

© Commonwealth of Australia 2014.

Australian Communications and Media Authority.

**ONLINE GROOMING**

Advice from **ThinkUKnow, a cybersafety website run by the Australian Federal Police**

Online grooming is when an adult makes online or phone contact with someone under the age of 16 with the intention of establishing a sexual relationship. This is a criminal offence and occurs in the communication, so you never have to meet this person face to face for them to be investigated and charged.

The people who ‘groom’ young people, we use the term online sex offenders, may pretend to be someone your age, but often are upfront with the fact that they are an adult and quite older than you. They can manipulate you and make you feel as though your relationship with them is special.

The first thing to realise about this kind of relationship is that it is wrong. Adults who pressure young people into doing anything that they don’t feel comfortable with should be reported to the police and blocked. They can be very clever and make you feel as though you have to do something because you owe them, or because otherwise they will get you in trouble.

This is wrong and you should report them. You won’t get into trouble for reporting someone like this, no matter what you’ve done.

**So what can you do about it?**

- If you think you’re being groomed or an adult has approached you online for sex, you should report it to the Australian Federal Police at www.thinkuknow.org.au/site/ocse.asp
- Only accept friend requests from people you know and trust.
- If you’re speaking to people you don’t know, avoid using your real name or sharing any personal information such as your age or contact details.
- Never use a webcam with someone you don’t know.

Tip 1: Make sure your profile is set to private

To manage your privacy on social media such as Facebook, Twitter or Instagram, you have the option of making your profile either private or publicly accessible. You can check this through the Settings option on your profile and/or accounts.

People aren’t always who they say they are. Before you accept a friend request from someone, ensure that you know who they are offline.

Tip 2: Only accept friend requests from people you know and trust and learn to block offensive users

People aren’t always who they say they are. Before you accept a friend request from someone, ensure that you know who they are offline and that you trust them to protect the personal information you share on your profile. Just because you share a mutual friend, doesn’t mean you actually know the person.

If people harass or threaten you online, you can block them from communicating with you.

Tip 3: Regularly search for yourself online

Regularly search for your name, email addresses and any usernames you operate in online search engines such as google, Bing or Yahoo. You can also look up your name using www.pipl.com which brings back many social media results. Also try searching your name using the search functions on Facebook and Twitter.

These searches will allow you to identify fake profiles and/or accounts, as well as gain a better understanding of what your digital footprint looks like.

Tip 4: Report fake profiles

Fake accounts or accounts impersonating others on Facebook, Twitter and Instagram can be reported. Forms can be found on these social media sites which you can complete to report these incidences.

Tip 5: Do not join offensive online groups or ‘like’ offensive online content

Depending on your privacy settings, the groups which you belong to on Facebook can be publicly available information. Your name is then linked with the objectionable content shared on those Facebook groups, which you have no control over.

Tip 6: Do not post inappropriate content online

Think before you post any content online as it is impossible to permanently delete digital content once it has been shared.

Tip 7: Delete unused accounts

If you are no longer using your online accounts, it is best to deactivate or delete them.
Before you delete your accounts:

- Type your full name into a search engine such as google or www.pipl.com to find out which social media accounts you have. Also try searching your email addresses in these search engines. You may have an old Myspace or Bebo profile which you’ve forgotten about, but this could still contain personal information or photos of you.
- Make sure you know your log-in details for each account. If you’ve forgotten which email address you used to start up the account, have a search in your email accounts for Facebook, Bebo, Myspace and Twitter to see which email account is linked to each profile.
- If you have forgotten the password to access your social media accounts, follow the directions in the ‘Help’ or ‘Safety’ section of the social media website to find out how to recover a forgotten password.
- Have a look at the photos on your profile in which you’re tagged. Photos uploaded by friends will still be available after you’ve deleted your account. Contact your friends and ask them to remove these photos and, if they do not take them down, you can report the photo to the site on which it appears.

Facebook and Twitter give you the option of downloading a copy of all the information you have on your profile including photos, comments and your wall posts. Before deleting your account, it’s a good idea to keep a copy of your information for your own records, but also to make sure you don’t lose any of your photos.

**Do not generate, accept or forward on any naked images on your phone or online of someone who is under the age of 18 as they may be considered child pornography.**

**Tip 8: Turn off your Bluetooth when not in use and change the name of your device**

Bluetooth creates a wireless network between paired devices within a limited range. There are ways in which vulnerabilities in Bluetooth can be exploited, providing access to your address book, calendar, messages, photos and other content on your mobile phone.

To reduce your exposure to this risk, ensure that Bluetooth is disabled or hidden when not in use and that the name of the device is changed to something which doesn’t identify you, or the model of the phone.

**Tip 9: Disable geotagging on your mobile device**

Geotagging is the process whereby data is added to an image or other content.

When this geotagged material is shared online, it is possible for others to read the metadata and identify the location where that image was taken.

Steps for disabling geotagging or location services for the camera on your smartphone can be found on page 18 of the Social Media Reputation Management booklet.

**Tip 10: Do not take, accept or forward nude images of someone under the age of 18**

Do not generate, accept or forward on any naked images on your phone or online of someone who is under the age of 18 as they may be considered child pornography. By having these images on your phone or computer you could be deemed as having possession of child pornography. Forwarding them onto others could also be considered to be distribution of child pornography. These are serious criminal offences which can carry gaol terms of up to 15 years. You should report these images to your local police.

A conviction of child pornography-related offences can have serious long term consequences including being placed on a sex offenders’ register and imprisonment.

---

PROTECTING PERSONAL INFORMATION

cyber[smart:] explains how your online personal information can be misused by criminals or inappropriately by marketers, and how you can manage the risks

Personal information is any information or combination of information that enables an individual to be identified.

**What is personal information?**

Personal information may include:

- Full name
- Address
- Phone numbers
- School
- Date of birth
- Email address
- Username and password
- Bank details.

Personal information is used responsibly online by many businesses for legitimate communication. However, this is not always the case and some personal information can be misused by criminals or inappropriately by marketers.

**Disclosing personal information online**

Many online services require users to provide some personal information in order to use their service. Prior to providing personal information, users should try to think about what can potentially be done with their personal information and assess whether they are still happy to pass on these details.

In addition to inappropriate or illegal use of information, disclosing personal information online can impact on the user’s digital reputation—the opinion that others hold about that person based on their online activities.

There are several online activities that may require a level of disclosure of personal information, these include:

- **Shopping**—to verify the identity of the purchaser, to process payments or for the delivery of goods.
- **Subscribing or registering**—a screen name or ID and an email address are often minimum requirements but other requested information may include: age, gender, address, photo and personal likes or dislikes. A red asterisk (*) generally identifies mandatory fields that are needed to register.
- **Competitions, prizes and rewards**—online competitions often require users to provide extensive personal data, including personal interests and demographic details. This is used by the promoters to develop their marketing strategies or products.
- **Online games and virtual worlds**—these may require registration details, which include personal information, before the user can begin to play.

**Potential implications of sharing personal information online**

Spam is a generic term used to describe electronic ‘junk mail’—unwanted messages sent to a person’s email account or mobile phone. This mail could be email, instant messaging, SMS and MMS (text and image-based mobile phone messaging) of a commercial nature. It does not include faxes, internet pop-ups or voice telemarketing. Under the **Spam Act 2003** it is illegal to send or cause to be sent unsolicited commercial electronic messages in Australia.

The content of spam messages varies from promoting products or services to containing offensive or fraudulent material and some spread computer viruses.

**Cookies**

Cookies are a web browser tool which store information related to browsing activity and reports this back to the website. Cookies are intended to allow websites to remember a user and save personal settings. Personal information may be collected and shared via the cookie. It is good practice to delete cookies on a regular basis.

**Fraud**

Internet-based fraud is organised and uses the anonymity of the internet to steal information and resources for financial gain. Simple fraud scams can seek money or personal details directly from targets, while others seek personal information from targets that will be misused to obtain money, resources or information by deceptive means.

**Identity theft**

Identity theft is a specific type of fraud that involves stealing money or gaining benefit by the perpetrator pretending to be someone else. It can be financially...
Scams

Scams are often sent via email but can be sent by instant messaging, SMS (text messages) and MMS (image-based mobile phone messaging). According to SCAMwatch, anyone can fall victim to a scam.

Scams succeed because they look like the real thing and scammers manipulate people into responding. Scams can appear to come from authoritative sources, like a well known bank or telecommunications provider. They may make people fearful that they will miss out on a special offer, or feel ashamed of themselves for denying access to the victim’s financial details such as credit card numbers, account names and passwords or other personal information.

- **Advance Fee (or ‘Nigerian 419’)** – These scams offer to pay a considerable sum of money to assist in transferring millions of dollars out of a foreign country for various legitimate sounding reasons. Similar to lottery scams, unexpected fees arise that must be paid before the money can be transferred.

- **Mule** – Prospective victims are sent attractive job vacancy adverts claiming to provide high pay for limited work. The job often involves transferring sums of money between accounts. This is money laundering and the victim themselves may ultimately face criminal charges.

**Actions to protect personal information**

It's important to understand how personal information is used online and how students can manage and protect their information and digital reputation. Schools can provide the following tips to parents, as well as the children and young people in need of guidance.

**Only disclose financial information on secure websites**

Credit card details, bank account details, tax file numbers, passwords or other personal information should never be sent electronically unless on a secure website. This may be indicated by a web address beginning with `https://` and a ‘locked’ padlock symbol in the bottom of the screen, which indicates that data is being encrypted.

If in doubt about the legitimacy of a website, call the organisation it claims to represent. When calling, do not use phone numbers provided on the suspect website or in suspect emails. Use a known phone number or one obtained from a trusted source such as the White or Yellow Pages or a government website. The SCAMWatch website provides further advice on how to identify and report potential scams.

**Providing information to your banking institution**

Banking institutions will never email individuals asking for their username or password. If you receive an email by an organisation claiming to represent a banking institution report the email to the bank and SCAMwatch. Do not respond and do not click on any links provided.

**Read user agreements and privacy policies**

Encourage students to read user agreements or privacy policies to determine how their personal information may be used in the future. Many organisations use information for marketing purposes and may sell it to other marketing firms. If information is posted on websites that do sell information to marketers, individuals may receive promotional spam emails which can be difficult to stop.
Reduce spam by protecting your details
Spam can be reduced by:
• Limiting disclosure of email addresses and mobile numbers
• Installing and using spam filtering software
• Checking the terms and conditions when purchasing products, entering competitions or registering for services or email newsletters
• Not allowing contact details to be used for marketing purposes
• Boosting online security to limit spam.

More information about spam and how to make a complaint is provided on the ACMA website, www.acma.gov.au

Set up an alternate email account for subscriptions and registrations
Use a separate address to communicate with friends, family and for work or study.
When entering competitions or subscribing to websites, an alternate email address can be generated using free webmail. These email accounts can be deleted easily, with little impact if spam becomes unmanageable.

Be selective about using your name in your email address
Setting up an email account name is one instance where students should be careful about the information that they share. For example, JackSmith13@hotmail.com reveals the users name and potentially his age whereas Jack@hotmail.com is fairly secure and does not reveal personal information.

Understand that information shared online can be permanent
Information posted and shared on social networking sites may be permanently recorded and users may not have control over who sees or accesses their personal information. This includes teachers, parents and prospective employers. When joining online communities, students are advised to read and understand the privacy policies and settings offered to prevent access to personal information, including images.

Select passwords carefully
When creating passwords there are some definite dos and don’ts, these include:

Do
• Make it at least eight characters in length
• Combine letters, numbers and upper and lower case letters
• Change your password regularly.

Don’t
• Use pet names, birthdays, family or friends’ names
• Share passwords with others, even with friends
• Store them on the device or write them down.

It’s important to change passwords regularly to ensure that all personal information is kept secure.

Managing the risks
There are a number of actions schools can take to educate students about the protection of their personal information. These include:
• Establishing a cybersafety contact person. This person would provide guidance to students and parents on issues concerning student safety and wellbeing.
• Educating students and parents about the appropriate use of personal information online, including a reference to information about protecting personal information in the school newsletter. Download: Common cybersafety issues – protecting personal information from www.cybersmart.gov.au
• Integrating the Cybersmart teacher resources into the school curriculum to equip students with practical cybersafety skills and knowledge.
• Booking an Outreach Professional Development workshop for teachers and Internet Safety Awareness presentation for students and parents. These are free to all schools.

Useful websites

Kids Helpline
Kids Helpline is free, anonymous and available 24/7 on 1800 55 1800 or via their website, www.kidshelpline.com.au

Budd:e
The Stay Smart Online website hosts the Budd:e Cybersecurity Education package, designed to raise cybersecurity awareness of primary and secondary school students. The Budd:e Cybersecurity Education Package consists of two activity-based learning modules, one for primary and one for secondary school students. Visit: www.budd-e.staysmartonline.gov.au

Stay Smart Online
The Australian Government’s cybersecurity website provides information for Australian internet users on the simple steps they can take to protect their personal and financial information online.
Visit: www.staysmartonline.gov.au

SCAMwatch
SCAMwatch is a website run by the Australian Competition and Consumer Commission (ACCC). SCAMwatch provides information to consumers and small businesses about how to recognise, avoid and report scams. Visit: www.scamwatch.gov.au

Office of the Australian Information Commissioner
Privacy is one of the three broad functions of the Office of the Australian Information Commissioner (OAIC). Visit: www.oaic.gov.au/index.html

© Commonwealth of Australia 2014.
Australian Communications and Media Authority.

Issues in Society | Volume 381
Online Safety
21
Secure your mobile phone and devices

The features that make your phone ‘smart’ also make it susceptible to viruses and malicious software. If your phone isn’t secure and it is lost or stolen, your personal information, including passwords, banking details, emails and photos could be used to access your money or to steal your identity. Following is security advice from the Australian Government initiative, Stay Smart Online

Mobile phones, especially smart phones are mobile computers. They allow you to access the internet and email, download applications and games and store personal contacts, photos and information. You need to protect and secure your phone just as you would your home or mobile computer.

**TOP TIPS**

- Put a password on your phone and a PIN on your SIM card. Do not rely on the default factory settings. Using a password and PIN will stop thieves getting access to your phone or using the SIM in another phone to make calls. All phones have security settings so familiarise yourself with them and turn them on.
- Setup your device to automatically lock. If your phone has not been used for a few minutes, it should automatically lock and require a password or PIN to reactivate.
- Encrypt your data. Some phones allow you to encrypt your data, sometimes using third-party software. Encryption secures your data if your phone is lost or stolen.
- Consider installing security software from a reputable provider. Anti-virus, anti-theft, anti-malware and firewall software is available for some mobile phone operating systems.
- Stay with reputable websites and mobile applications (apps). Always keep an eye on your commonly used websites’ addresses and make sure you are not redirected or diverted to other websites. When using any financial mobile applications, such as mobile banking, make sure to only use applications supplied by your financial institution.
- Be careful when allowing third party unsigned applications to access your personal information. This includes access to your location. Always read permission requests before installing new apps or app upgrades, looking for unusual requests or pleas for money.

Remember your smart phone is a computer – all the same security rules apply.

- Do not click on unsolicited or unexpected links. Even when they appear to be from friends.
- Check your phone bill for unusual data charges or premium rate calls. Contact your service provider immediately if you discover any unusual calls or data usage on your bill.
- Check for updates to your phone’s operating system regularly. Install them as soon as they are available.
- Be smart with Wi-Fi and Bluetooth. When connecting to the internet using Wi-Fi, try to use an encrypted network that requires a password. Avoid online banking or financial transactions in busy public areas and over unsecured Wi-Fi networks. Ensure that passers-by can’t watch what you are typing (known as shoulder-surfing). Turn Bluetooth off when you aren’t using it.
- Back up your data regularly. Set up your phone so that it backs up your data when you sync it, or back it up to a separate memory card.
- If you decide to recycle your phone, make sure you delete all your personal information first. Most phones have an option to reset to factory settings. Remember to remove or wipe any inserted memory cards.
- To assist you in case of your mobile theft or loss, ask your provider or manufacturer whether it has services such as mobile tracking and the ability to remotely wipe your information stored on the phone.

**REMEMBER IT’S NOT ‘JUST A PHONE’**

- Treat your smart phone like your wallet – keep it safe and on your person at all times.
• Remember your smart phone is a computer – all the same security rules apply. This includes checking the authenticity of websites, not clicking on links from people you do not know, and watching out for phishing scams (by email, text or even voicemail) asking for personal information.

SECURE YOUR PHONE

• Turn on the security features of your phone. All phones have security settings, so familiarise yourself with them and turn them on.
• Many mobile phones allow users to set a password or Personal Identification Number (PIN) that must be entered to use the phone. Passwords and PINs make it more difficult for thieves to steal your personal information if your phone is lost or stolen.
• Put a PIN on your SIM card and password on your phone so that thieves cannot steal your phone credit or run up your phone bill.
• Consider installing security software from a reputable provider. Anti-virus, anti-theft, anti-malware and firewall software is available for some mobile phone operating systems. Check with your phone manufacturer for recommendations.
• Check for updates to your phones operating system regularly. Install them as soon as they are available – these updates often contain changes that will make your phone more secure.
• Bluetooth lets you wirelessly connect to devices and transfer information over short distances. For Bluetooth to work, devices need to see each other and then connect. It is best to leave your phone in undiscoverable mode (hidden) so that it is only visible when you specifically need other people or devices to see it. This means that hackers cannot easily see your phone and they cannot easily connect to it unless they already have your Bluetooth address. When connecting using Bluetooth, do so in private, uncrowded areas only.
• Be smart with Wi-Fi. When connecting to the internet using Wi-Fi, try to use an encrypted network that requires a password and which you are sure is operated by a reputable provider. Read our tips for using public wireless networks at www.staysmartonline.gov.au
• Change your settings so that your phone asks permission to join a new wireless network.

SECURE YOUR INFORMATION

• Encrypt your data. Some phones allow you to encrypt the data stored on your phone or memory cards, sometimes through the use of third-party encryption products. Encryption secures your data if your phone is lost or stolen.
• Back up your data regularly. Set up your phone so that it backs up all your data each time you synchronise with a computer. Alternatively, backup your device to a memory card regularly and keep it in a safe place.
• Do not save passwords or PINs as contacts on your phone unless you encrypt them properly. With all the PINs and passwords we have to remember, it is tempting to save them in your phone as fake contacts in case you forget them, but this can lead to a compromise if you lose your phone or the data in it is stolen.

• Avoid online banking in busy public areas. Passers-by could be watching what you are typing (known as shoulder-surfing).

Think carefully about what information you and your phone shares online and how it could be misused.

STAY WITH REPUTABLE WEBSITES AND MOBILE APPLICATIONS (APPS)

• If your phone allows you to run applications downloaded from the internet, make sure you understand the risks that your personal information including your location, contacts and messages can be breached if the permissions for mobile applications are not set up properly.
• Most smart phones allow you to control your personal information accessed by the mobile applications by choosing permissions at the time of installation.
• Do not get led into the trap of downloading hoax or malicious software that could contain a virus or malware.
• Think carefully about what information you and your phone shares online and how it could be misused. Your smart phone holds a great deal of personal information in a single place, making the job of fraudsters very easy. So it’s not just about what you put on your social networking profile, but also that it’s probably easy to work out who you bank with, where you’ve recently made transactions, the names of your family and to glean other details from emails or other documents.
**MOBILE PHONE RISKS**

**High bills** – children and young people may not consider the impact of their mobile phone use, or the cost of premium services, like ringtones or games, which are more expensive than a standard SMS.

**Scams** – young users may also be more susceptible to mobile phone scams that are designed to steal personal details or money. Children may not know they’ve been scammed unless invoices or online statements are checked carefully for unusual charges.

**Cyberbullying and unwelcome mobile calls** – mobile phones are often used for cyberbullying, as they are easy tools for bullies to use. Mobiles can also be used to make calls that are threatening, offensive or harassing in nature.

**Sexting** – a growing issue is young people’s use of mobile phones to send sexual images to one another. This can have social and legal consequences.

**Access to inappropriate material** – internet-enabled mobiles allow children and young people ready access to a range of material that their parents may consider inappropriate for them.

---

**PLAN AHEAD**

- Note down the details of your phone in case of theft. Every phone and cellular capable tablet has a unique International Mobile Station Equipment Identity (IMEI). Most phones allow you to find out your own by keying in *#06#. Knowing this number will help your network provider to stop your phone being used if it is stolen.
- If you lose your phone or it is stolen, report it to your network operator immediately so it can be disabled. If you find it again you can easily re-enable the phone.
- To assist you in case of mobile theft or loss, ask your provider or manufacturer whether it has services such as mobile tracking and the ability to remotely wipe your information stored on the phone.

---

**BE SMART ABOUT HOW AND WHERE YOU USE YOUR PHONE**

- Turn Bluetooth off when you aren’t using it. Bluetooth lets you wirelessly connect to devices and transfer information over short distances. For Bluetooth to work, devices need to see each other and then connect. It is best to leave bluetooth off until you are using it or put your phone in undiscoverable mode (hidden) so that it is only visible when you specifically need other people or devices to see it. This means that hackers cannot easily see your mobile phone and they cannot easily connect to it unless they already have your Bluetooth address. When connecting using Bluetooth, do so in private, uncrowded areas only.
- Stick with reputable sites and applications when downloading applications from the Web. Many mobile phones include internet browsers that let you surf the web and download content to the phone.

---

Do not download content, particularly applications, from unknown or unreliable sources. They could contain malicious software. Use the application store or website of your mobile phone operating system or manufacturer.

- Turn GPS off when not using it. While GPS can provide great benefits in finding out where you need to go, it can also be used by others to see where you or your phone is located.
- Log out of websites when you are finished. It can be tempting to stay logged into a website to save time or so the site can remember your password. It is best not to do this because if your phone is stolen or lost, a user can access your account.
- Think before you click. Do not open multimedia messages (MMS) or attachments in emails, or click on links in emails and SMS messages unless you are expecting them and they are from a trusted source. They could contain malicious software or take you to a malicious website.
- Change your settings so that your phone asks permission to join a new wireless network.

**While GPS can provide great benefits in finding out where you need to go, it can also be used by others to see where you or your phone is located.**

---

**PROTECT AGAINST MALICIOUS SOFTWARE**

- Watch out for prompts or warnings asking if you want to allow software to install or run – if you do not know what it is or what it relates to, err on the side of caution. Criminals sometimes try to dupe users into downloading malicious software (often referred to as ‘social engineering’).

---

**SYMPTOMS OF MALICIOUS SOFTWARE INFECTION**

Your phone may have been infected with malicious software if any of the following things have happened:

- There is a sudden large increase in your phone bill with no clear reason
- Your phone has emails and messages in the sent folder that you did not send, or
- The user interface has changed without you taking any action to change it.

Contact your service provider for instructions on how to identify and remove malicious software.

---


This e-book is subject to the terms and conditions of a non-exclusive and non-transferrable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: St Mark’s Anglican Community School, Hillarys, libraryadmin@stmarks.wa.edu.au
Sexting is when sexual photos or videos are shared via mobiles or online posts. If your child has been involved in sexting, there are things you can do to help them manage the situation, according to this fact sheet from cyber[smart:]

Teens are on show – their mistakes are public

Our children’s mistakes may become public fodder. This is not because we have raised them badly, but simply because the technology allows it. This is quite different to our childhood.

So you got naked online
Managing sexting with your teen. This resource helps teens understand what to do when their naked image is posted online. Download So you got naked online from www.cybersmart.gov.au/Parents/Cyber%20issues/Sexting.aspx

Aussie teens and sexting infographic
What are Australian teens doing with sexting and naked pictures. This infographic lays out some interesting findings. Download Aussie teen and sexting and view infographic from www.cybersmart.gov.au/Parents/Cyber%20issues/Sexting.aspx

Why did they sext?
Researcher Danah Boyd says teens share images for all kinds of reasons ... to express developing sexuality, to impress or be liked and to keep up with what they think is the norm.

Most images are shared within relationships and most teens don’t expect images to be shared with others, with the exception of a few who hope they will gain fame. www.danah.org/papers/talks/2011/RWW2011.html

How do I support them?
If their image has been viewed by others they may be publicly bullied and have sexually inappropriate comments made about them by friends and strangers, including adults.

Providing support will help buffer the impact of bullying. Keep them connected to trusted friends and family online and offline. Stop them reading offensive comments. Keep an eye on them and get others to do so as well. If you are worried or your child is vulnerable, seek professional support.

Minimising the spread of images
Unfortunately once shared online, many images end up on sites that are used for adult gratification. Act fast to help prevent this.

If schoolmates are involved the school may be able to help.

Help your teen identify where the images might be and send take-down requests to all sites.

Send messages to all kids who may have received an image asking them to delete immediately.

Help them block any people who make offensive comments about them and report them to the police if necessary.

The law
While it can be a crime to take and share sexual images of people under 18, the police don’t usually prosecute if there is no harm to those involved.

They are more likely to get in trouble with the law if they have deliberately shared a photo or video of someone without their consent, especially if they meant to embarrass or humiliate them.

If the police get involved they will want to know how the image/video was made and where it might have been sent/posted. They will want to know who was involved and whether there was consent from all involved. Help your child put together a record of what happened and where images and videos might be.
Warning signs – don’t ignore them

- If your child’s behaviour changes at home and/or school you should talk to them. Examples of worrying changes include seeming less interested in things they used to like, not connecting with friends as they used to, seeming more withdrawn, appearing unhappy a lot of the time, changed eating and/or sleeping (more or less of either). If your child seems to think poorly of themselves act straight away. Seek professional advice if necessary including through the school counsellor, your GP or a psychologist.
- If your child has particular vulnerabilities, be vigilant about their contacts offline and online. Help them join groups out of school where they can find friends and support. Talk to the school and make sure they are supported.
- Headspace and Lifeline on 13 11 14 also provide free counselling and support.

Where do I go for help?

School support
If you are concerned about your child’s involvement in a sexting incident, their school may be able to help. For more information, contact your child’s school.

Counselling
- Kids Helpline
  Kids Helpline provides free, confidential online and phone counselling for 5-25 year olds. 1800 55 1800 kidselpline.com.au
- eheadspace
eheadspace is for 12-25 year olds in need of support or worried about their mental health. 1800 650 890 eheadspace.org.au
- Cybersmart Outreach internet safety awareness presentations
  Cybersmart Outreach offers free internet safety awareness presentations for parents, students and teachers. These sessions are informative, non-technical and available to all schools. Ask your child’s school if they have registered to host a parent presentation.

© Commonwealth of Australia 2014.

The recent story of an Adelaide mother who is struggling with her 17 year old son’s addiction to the online fantasy game Runescape probably rang alarm bells with many parents who suspect or know their teenager is in front of a screen far too often and for far too many hours at a time.

Research shows that in America 97% of all children play video games and 2% are addicted*. According to the Entertainment Software Association (ESA) in the USA 25% of players are under 18 years of age and 60% are male.

The American Psychiatric Association will add ‘internet use disorder’ to the research appendix of its Diagnostic and Statistical Manual of Mental Disorders (DSM-5) in May 2013. Dr King, researcher at the Adelaide University School of Psychology said “this is the first time internet-related disorders will be acknowledged in the DSA.”

Writing in the latest issue of the Royal Australian and New Zealand Journal of Psychiatry, Dr King confirmed that mental health experts are debating whether to define the illness as ‘internet addiction’ or ‘video gaming addiction’.

Research shows that in America 97% of all children play video games and 2% are addicted.

THE 5 TELL-TALE SIGNS OF ONLINE GAMING ADDICTION

- Pre-occupation with gaming and hiding gaming use
- Social withdrawal or isolation
- Disengagement from school life
- Loss of interest in other activities
- Defensiveness and anger.

TIPS ON HOW TO HELP TEENS WITH A GAMING ADDICTION

1. Parent tag team: it is important that both parents take the addiction seriously and back each other up. They must approach their child together so that the child knows they cannot divide and conquer their parents by playing one off against the other in an effort cover up their addiction, appealing to the weaker parent for support only enables the child to continue and to some extent hide their game playing from the other parent.

2. Encourage educational games: there are plenty of games that have an education base, encourage a child to play these instead of violent online games. There are also websites that engage players with other players from around the world to see who can complete educational tasks, like
maths problems, the quickest. The participants are given points and can progress to different levels. It can give the player the same sense of empowerment, satisfaction and achievement as online commercial games.

3. **Set time limits:** parents need to establish clear time limits with a child. Enter into a contract if necessary. Sit down with the child and discuss what is a reasonable amount of time to play a game, by involving the teenager in the decision making process, they are more likely to adhere to the boundaries set.

4. **Look for the school connection:** is a child turning to online games because they are not doing well at school? It is hard to tell what comes first: the poor marks or the online games. Not performing well at school impacts a child’s self-esteem. They may retreat more into the game to cope with negative feelings about themselves. At least in the virtual world they can control things. Try to encourage their studies and find out if they are finding any areas difficult.

* Pew Internet and American Life Project, USA.

Source: The American Journal of Family Therapy. ‘Understanding Online Gaming Addiction and Treatment Issues for Adolescents’ by Kimberly Young.

---

You can gamble online any time and anywhere – at home, at work, on your phone when you’re out. Gambling this way might feel more comfortable and less risky than gambling at a venue. But the fact is, it can be just as easy to spend more time and money than planned.

Even if you only gamble what you can afford, online gambling can affect other parts of your life. Unknowingly, the time spent gambling online can affect your job, your personal relationships with friends and family, and even your health.

**Losing track**

It is easy to ‘zone out’ when gambling online. After a while, time and money are gone and we don’t really remember how it happened.

Betting with credit or a linked account instead of actual cash can make it feel less real – like it’s not even really money we’re gambling with.

Being alone means there is no one to talk down a bigger bet, to remind us to slow down or take a break, or to support us after a loss.

**Tips for avoiding problems**

- Set a limit for yourself on how much you will spend.
- Calculate how long you had to work to earn that money.
- Use a site that has limits on daily spend.
- Limit where you bet, don’t have multiple accounts.
- Use a debit card instead of a credit card – this will help you see that it is your income you are spending.
- Check your player history on the sites you use and/or your bank and credit card statements to keep a clear idea of how much you are spending.
- Read the fine print on marketing promotions like ‘free bets’.
- And remember, like any form of gambling, online poker, betting and sports wagering is not a good way to make money.

**Practice sites**

Some sites offer free games so that people can ‘practice’. Be aware that the odds on ‘practice’ games are much better – so it is easier to win than on the paid games. When winning at the practice games don’t expect to have the same results in the paid games.

**Offers and promotions**

Because what you do on websites can be seen and tracked by the website owners – how often you visit, what you spend, how your gambling patterns may change – they can use this information to market to you very effectively. They can send you bonuses and offers to keep you gambling and promotions to come back to their site if you haven’t bet in a while.

You can gamble online any time and anywhere – at home, at work, on your phone when you’re out.

**How problems develop**

- Just filling free time with gambling
- Continually adding money to one or more online accounts, without making withdrawals
- A few small bets here and there and then one day it just snowballs
- Having a win from that first bet and thinking that it’s easy money
- Having an urge to try and get money back
- Betting without caring about the outcome
- Winning and then spending it all very quickly.

**Signs of a problem**

- Disrupted, or not enough, sleep
- Debts starting to mount up
- Not being able to pay bills
- Bigger bets placed to get the same feeling
- Betting when you normally wouldn’t, like during lunch breaks
• Missing school or work
• Thinking about gambling, when doing other things.

**What you can do if you have a problem?**
• Block yourself from receiving free offers, incentives and other marketing materials from gambling sites
• Most reputable sites offer self-exclusion programs
• Block gambling sites from your computer – you can do this yourself or install software that filters out gambling websites. Asking a trusted support person to set this up for you will help you avoid the temptation to remove the filter
• Take betting apps off your phone
• Get help.

It is easy to ‘zone out’ when gambling online. After a while, time and money are gone and we don’t really remember how it happened.

**How do you know a site is safe?**
• Wagering and sports betting is legal in Australia. Australians can bet at offshore casinos however it’s illegal to provide online casino facilities from Australia
• If you gamble at an offshore site there are fewer regulations and safeguards
• People have won money at offshore sites only to find that their stake was stolen, they never saw their winnings and the site has been shut down
• Go to sites that have some accreditation. This might be from eCOGRA who check the integrity of the provider.

**Your questions**

*If I use the betting exchange agencies, won’t I have a better chance of winning?*

The bottom line is that over the long run the operator is always going to win and the punter is always going to lose. Betting exchanges can seem like a good deal. They take a commission on wins and are set up so that punters are betting against each other. But someone always has to lose for every win. Whether you win or lose you are still paying the betting exchange money. That’s how they are successful.

*I’m the best poker player that I know, I see people on TV making lots of money playing poker professionally, couldn’t that be me?*

It is true that there is a strong element of skill in poker and some people can manage to play professionally and routinely come out ahead. Professional poker players play online in a very controlled manner and they do not chase their losses or bet more than they can afford. When playing online you are in competition with millions of players around the world who are waiting to take someone else’s money. For someone to win, others have to lose. Even if you do play with perfect strategy, the cards are still chance and even the best players can and do lose.
Illegal and offensive online content is regulated through the Online Content Scheme under Schedule 5 and 7 of the Broadcasting Services Act 1992 through a complaints-based mechanism. The Scheme is designed to protect consumers, particularly children, from exposure to inappropriate or harmful material.

The Scheme applies to content accessed through the internet, mobile phones and convergent devices, and applies to content delivered through emerging content services such as subscription-based internet portals, chat rooms, live audio-visual streaming, and link services.

Under Schedule 7, prohibited content includes content that has been classified or is likely to be classified:
- RC (refused classification)
- X18+
- R18+ unless it is subject to a restricted access system
- MA15+ and is provided on a commercial basis (i.e. for a fee) unless it is subject to a restricted access system.

These prohibitions are backed by strong sanctions for non-compliance including criminal penalties for serious offences.

Where content is hosted in Australia and is found by the Australian Communications and Media Authority (ACMA) to be prohibited, the ACMA has the authority to direct the relevant content service provider to remove the content from their service. Where content is not hosted in Australia and is prohibited, the ACMA will notify the content to the suppliers of approved filters, so that access to the content using such filters is blocked.

In addition, regardless of where the content is hosted, if the ACMA considers the content to be of a sufficiently serious nature, it must notify the content to an Australian police force.

Schedule 7 includes a complaints-based mechanism administered by the ACMA. Information, including instructions for making a complaint to the ACMA, is available at the ACMA Hotline website, www.acma.gov.au

Complaints may be lodged by fax to (02) 9334 7799, by emailing online@acma.gov.au

See also the ‘Voicing your concern’ page at www.communications.gov.au/television/voicing_your_concern for a summary of the procedures for making a complaint about content on the internet, television and radio.

CONTACTS
Australian Communications and Media Authority
Queen Victoria Building NSW 1230
Tel: 1800 22 6667 (free call) or 02 9334 7700
Fax: 02 9334 7799
Free call: 1800 22 6667
www.acma.gov.au

ONLINE CONTENT COMPLAINTS

The Australian Communications and Media Authority can investigate a range of online content, including offensive imagery of children, material that advocates the doing of terrorist acts, content that incites, instructs or promotes in matters of crime or violence, as well as sexually explicit material.

The ACMA Hotline is a place where Australian residents can make a complaint about material that may be prohibited offensive or illegal online content (such as child sexual abuse material and material that advocates the doing of terrorist acts).

You can report offensive or illegal online content to the ACMA Hotline via the online complaint form on the ACMA website.

NOTE: If you believe that a child or any other person is in IMMEDIATE danger, please contact the police on Triple Zero (000).

MAKING A VALID COMPLAINT

The ACMA can investigate content provided by:
1. Hosting services – includes stored internet content, postings made to forums and newsgroups, files accessible from peer-to-peer (P2P) applications and content delivered to mobile phones.
2. Live content services – includes live streamed video and audio content available online and on mobile phones.
3. Links services – includes links with access to other websites containing prohibited or potentially prohibited content.

Before you complain, ensure you answer yes to the below four statements:
1. I am an Australian resident or company that has activity in Australia.
2. I can give precise details so that the ACMA can access the online content.
3. I am satisfied the content is prohibited, that is, offensive or illegal (and meets the criteria on the Prohibited online content page of the website).
4. I can (briefly) indicate why I think the online content falls within one of the above prohibited classifications.

If you answer yes to the above statements, go to the online complaint form to start the complaint process.

If you cannot access the online complaint form, you can email your complaint to online@acma.gov.au, fax it to (02) 9334 7799 or mail it to:

The ACMA Hotline
Australian Communications and Media Authority
GPO Box Q500
Queen Victoria Building NSW 1230

Please note that under no circumstances should printed or electronically stored images of content be forwarded through the post. Supplying the access information and the other details noted above is enough to enable the ACMA to conduct an investigation.

For further information about the ACMA Hotline or to make a complaint about online content see:
• ACMA Hotline online complaint form
• ACMA Hotline FAQ
• Online content investigation statistics.

Australian Communications and Media Authority.
Online content complaints (Last updated 22 May 2014).
CHAPTER 2
Dealing with cyberbullying

ENHANCING ONLINE SAFETY FOR CHILDREN

Following is the introduction from a discussion paper released by the Department of Communications aimed at tackling the growing scourge of cyberbullying among Australia’s children and young people.

THE DOMINANCE OF INTERNET USE AND SOCIAL MEDIA

The internet has become a daily, integrated part of life for many Australian families. It is an essential tool for all Australians, an integral part of our economic and social activities, and a vast resource of information, education and entertainment. The ability for young Australians to use online tools effectively provides both a skill for life and the means to acquire new skills. The internet provides children with a means through which they can exchange information, be entertained, socialise, do school work and conduct research.

Studies show that over 95 per cent of young Australians use the internet regularly. Almost daily internet use is common for children as young as eight or nine. This rapidly changes in the ‘tween’ years with many 10-12 year olds using the internet from 1-3 hours per day. By 13, social media use has become the norm; and by 15, the internet and its use has become an ‘organic integrated part’ of the everyday lives of Australian children.

Almost daily internet use is common for children as young as eight or nine. This rapidly changes in the ‘tween’ years with many 10-12 year olds using the internet from 1-3 hours per day. By 13, social media use has become the norm; and by 15, the internet and its use has become an ‘organic integrated part’ of the everyday lives of Australian children. Whilst the popularity of various online activities – including email, games, chat, shopping, and passive consumption of music and videos – varies with different age groups, social media use has grown dramatically to overtake other forms of online entertainment and communications used by Australian children.
In 2011, the use of social media was identified as the primary form of digital communication between young people over 13, overtaking more traditional digital means such as text messages, phone calls and email. While around half of young Australians aged between 8 and 11 years use social media sites, this figure dramatically increases to around 90 per cent for 12 to 17 years olds. Research on the specific social media usage habits of children and young people indicates that the small minority of 12-17 year olds that do not have a Facebook account (usually due to parental control) felt that they suffer a degree of social isolation and exclusion. 

This increased exposure to the internet and social media is also enhanced with the increase in ownership of internet-connected mobile devices, with research indicating that:

- 53 per cent of children own or access their first internet-connected device before 10 years old, and
- Around half of 14-17 year olds access the internet through mobile phones, with 43 per cent of them having their own smartphone.

The growing number of Australian children accessing the internet and social media through mobile devices is significant and highlights the capacity for children’s internet activities to, in some instances, occur ‘under the radar’ of parents, teachers and other supervising adults. In this new digital environment, with more children independently using the internet and social media, the government is seeking to address the online safety risks, such as cyberbullying, that are also increasingly affecting Australian children.

A recent study into cyberbullying in Australia published in the *International Journal of Children’s Rights* defines cyberbullying as “any communication, with the intent to coerce, intimidate, harass or cause substantial emotional distress to a person, using electronic means to support severe, repeated and hostile behaviour”. Cyberbullying can occur in a variety of ways, through a range of digital devices and mediums, most commonly smartphones and social media sites. On social media sites cyberbullying can be content-driven, such as posting embarrassing or harmful photos, videos, or rumours relating to an individual. These are often exacerbated by other social media features (such as ‘comments’, ‘shares’ and ‘likes’) which serve to actively promote and spread the harmful content at a rapid rate, and to a wide audience.

The Australian Communications and Media Authority’s (the ACMA) research indicates 4 per cent of 8-9 year olds; 21 per cent of 14-15 year olds; and 16 per cent of 16-17 year olds reported being cyberbullied. Other studies indicate that 53 per cent of teens have been exposed to cyberbullying, but with only a fraction of those children choosing to tell their parents.

Some of the more extreme cases of cyberbullying have resulted in young children committing suicide. Queensland’s Commissioner for Children and Young People and Child Guardian presented findings into cyberbullying and youth suicide in May 2013 which demonstrated that cyberbullying is one of the range of risk factors associated with youth suicide, with victims of cyberbullying possessing vulnerability characteristics known to be present in suicide deaths. The study showed that youth suicide statistics linked to bullying in Queensland alone were grim, and various advocacy organisations, including the Australian Human Rights Commission, have called for more serious treatment of cyberbullying as an issue harming the welfare of Australian children.

Media articles have reported the following instances:

- In September 2013, a Tasmanian 15-year-old schoolgirl took her own life after being bullied, including cyberbullied;
- A 13-year-old Sydney girl took her own life in April 2013 after bullies relentlessly pursued her;
- A 14-year-old Melbourne schoolgirl took her own life in January 2012 after suffering bullying unknown to her parents; and
- In 2009, a Melbourne mother blamed her 14-year-old daughter’s suicide on the internet and the tragic case has highlighted the problem of cyberbullying among young people.
Prior to the federal election in September 2013, the Coalition released its *Policy to Enhance Online Safety for Children*, with a view to specifically address these risks in relation to children, so that content and cyberbullying concerns are handled faster; children can quickly access assistance with online safety concerns; Commonwealth criminal laws relating to cyberbullying are appropriate and effective; and there is clear and expert leadership in online safety.

The policy sets out the commitment to:
- Establish a Children’s e-Safety Commissioner to take the lead across government in implementing policies to improve the safety of children online
- Develop an effective complaints system, backed by legislation, to get harmful material down fast from large social media sites, and
- Examine existing Commonwealth legislation to determine whether to create a new, simplified cyberbullying offence.

This discussion paper outlines aspects of these commitments for consideration. The Department invites comments on the policies outlined in this paper, as well as discussion of the specific questions posed in each chapter.

Regulatory measures in this area must of course take account of the underlying importance of freedom of expression to the Australian community. If measures proposed have the potential to impact on freedom of expression, then it is important that they are reasonable and proportionate to the intended policy goal of improving the online safety of Australian children.

**NOTES**

1. Young and Well Cooperative Research Centre, *Using technology safely and effectively to promote young people’s wellbeing*, March 2013, pg. 2.
2. Australian Communications and Media Authority, *Like, post, share: Young Australians’ experience of social media – Qualitative research report*, August 2011, pg. 15.
5. Australian Communications and Media Authority, *Like, post, share: Young Australians’ experience of social media – Qualitative research report*, August 2011, pg. 23.
7. Australian Communications and Media Authority, *Like, post, share: Young Australians’ experience of social media – Quantitative research report*, 2013, pg. 22.
9. Definition of cyber-bullying contained in *Megan Meier Cyberbullying Prevention Act* Sec 88'(a), cited in Srivastava, Gamble & Boey, *Cyberbullying in Australia: Clarifying the* 

---

Cyberbullying can occur in a variety of ways, through a range of digital devices and mediums, most commonly smartphones and social media sites.


This is the second report of a three-part series researching the youth exposure to cyberbullying in Australia, commissioned by the Department of Communications.

The objective of this part of the research was to ascertain the estimated prevalence of cyberbullying incidents involving Australian minors that are reported to police, community legal advice bodies and other related organisations, the nature of these incidents disaggregated by broad socioeconomic categories and categories of cyberbullying behaviours, and how such incidents are currently being dealt with.

This research draws from a wide range of data sources: an online survey of stakeholders, qualitative interviews, a case study, a review of other research commissioned by the Department, and a review of how police respond to and record such incidents. The research provides a clear picture of the way cyberbullying is reported, dealt with and recorded by the relevant authorities, and a view about the strengths and weaknesses of the current system.

**CASES OF CYBERBULLYING REPORTED**

A large proportion of cases of cyberbullying are reported to schools. It is not possible to accurately identify the percentage of incidents which are reported to schools: the best estimate is that about half of incidents involving secondary school students are reported to schools. The incidence of reporting in primary schools was much lower than secondary schools, with only a tenth of the rate of reporting.

Young people in their early teens (13-15 years old) are most likely to be reported as victims of cyberbullying. It also appears that by the age of 15 or 16 years old, young people are more aware of their online behaviour and also more aware of protective behaviours. Thus the incidence of reports of cyberbullying reduces in the late teens along with the reduction of cyberbullying incidences.

The majority of victims of cyberbullying reported to organisations are female, but there are mixed findings in relation to the gender of cyberbullies, with some organisations reporting mainly male bullies and some reporting equal proportions of male and female cyberbullies.

The research found an apparent discrepancy between the number of cases which schools report to police and the number of cyberbullying cases recorded by the police. This appears to be a consequence of the way police categorise reports, with cyberbullying currently not being identified in either the allegation or the Modus Operandi, and of the way police generally respond to reports by providing assistance or other informal diversionary options.

Legal advice bodies and other agencies tend to deal with complex cases. They receive referrals from a wide range of sources including victims and their families, as well as other organisations including police and schools.

Different organisations tend to respond to different types of cyberbullying reports. Schools tend to receive more complaints about text messages, emails etc., whereas other organisations tend to receive complaints involving social media. Incidents involving social media appear to account for the majority of incidents overall.

More females than males were reported to schools as being cyberbullies, but males appeared to be involved in the more significant incidents. The peak age of cyberbullies was 10-15 years old, with a large drop off of students reported as being cyberbullies who were older than 15 years old.

Most stakeholder groups indicated that reports of cyberbullying are increasing, with some organisations seeing sharp increases in reports in the recent past. However, the actual rate of increase is not possible to quantify. There are a number of possible reasons for this increase, but the most likely explanation is the increasing access by children and young people to the internet and smartphones, and their increasing propensity to use online methods to communicate.

**HOW CYBERBULLYING IS DEALT WITH**

Schools tend to deal with cyberbullying by mediating between the victim and bully, involving parents, and punishing bullies. Most schools have a cyberbullying policy or code of practice and include education about cyberbullying as part of the curriculum. When they do refer externally, schools tend to refer to the police.

The legal aid centres, ombudsmen and other service providers tend to take a restorative justice approach, providing support to both victims and bullies. This is especially salient given that many children are both victims and bullies. Agencies also provide advice and information to victims about their legal rights and the processes for protecting themselves, e.g. asking social network sites to take down offensive material.

Police only take formal action under youth offender legislation in the more serious cases; police will almost always use diversionary approaches such as warning the bully or, in very serious cases, using diversionary approaches such as juvenile justice conferences. In serious cases police may encourage victims to take out an Apprehended Violence Order (AVO) or request a
Prevalence of cyberbullying involving Australian minors

- Recent Australian studies suggest that a conservative prevalence for being cyberbullied would be in the vicinity of 20 per cent of children aged 8-17 years in a 12-month period. This estimate takes into account the varying methods and samples used in the Australian studies examined for this report. This gives a rough estimate of the number of children involved in cyberbullying as somewhere between 460,000 and 560,000 children in a 12-month period.
- This finding is within the estimates of other international studies which ranged in prevalence from 0.9 per cent 72 per cent, with reviews of published studies indicating an average of around 24 per cent. Most estimates indicate that rates of cyberbullying are still lower than rates of traditional bullying. However, there are also indications that Australia has higher rates of cyberbullying than European countries due to the higher levels of internet use of Australian children.
- The Australian studies also confirm international research evidence which indicates that cyberbullying is most prominent among middle-school aged youth (10-15 years). The studies suggest an inverse U-pattern: starting at low levels before the teenage years, increasing until mid-teens years, and then beginning to decrease over time. However, little is known about when children start cyberbullying or whether the age at which cyberbullying starts is changing over time.
- Findings are inconsistent, internationally and in Australia, regarding the gender balance of cyberbullies, with some studies indicating more girls engaging in cyberbullying behaviour whereas others show cyberbullying by boys to be more prevalent. Gender seems to be a function of the type of cyberbullying behaviour; some devices, methods of cyberbullying, and social networking platforms, are more preferred by girls whereas others are more preferred by boys. Girls appear to be more likely to be victims in Australian and international cyberbullying studies.
- Internationally and in Australia it is recognised that there is significant harm associated with bullying and cyberbullying. Studies have found that it is more than just hurtful name calling and can lead to serious psycho-social and life problems.
- There is some evidence in Australia and internationally that cyberbullying has increased over the past decade. However, the reasons for this are not clear. It could be an artefact of the higher levels of use of technology, the increased availability of smart phones, the shift from response-based interactions (text) to user-design and created (multi-media), or the elevated awareness of cyberbullying as a contemporary behaviour. Alternatively, the apparent increase may arise from the methods used to measure prevalence such as the timeframe used, how the question was framed, and whether a definition of cyberbullying was provided.
- Internationally, responses to cyberbullying incidents have involved strategies at the individual, school and parental level, and categorised as three approaches: reducing risk (prevention); combatting cyberbullying (technical and practical strategies/interventions); and strategies which buffer the negative impacts of cyberbullying (emotional coping and emotional support).
- In Australia, responses to cyberbullying most commonly include telling teachers and family members, and blocking or ignoring the cyberbully. As children age they are less likely to tell parents, and more likely to seek support from independent, anonymous and/or online sources.
- Australian parents’ responses to cyberbullying include speaking to or educating the child (most commonly), blocking the cyberbully, doing nothing, informing the school, contacting the parents of the cyberbully, and restricting the child’s use of the computer or mobile phone.
- Australian teachers most commonly respond to cyberbullying by informing and involving parents, engaging in counselling with all parties involved, and by the use of warnings or class discussions. The involvement of police was only marginally less common a response than warnings and class discussions.
- There is increasing understanding of how young people, parents and teachers respond to cyberbullying incidents in Australia. However, there is still a gap in our knowledge about the effectiveness of those responses.

© Commonwealth of Australia 2014.


This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: St Mark’s Anglican Community School, Hillarys, libraryadmin@stmarks.wa.edu.au
Online Safety

Cyberbullying is any kind of bullying or harassment done using technology. It really sucks because it can be public, hard to take down, or affect you at home. There are a lot of things it could be, and it can affect people in a lot of different ways.

Take five minutes to skill up on how to protect yourself, with this fact sheet advice reproduced courtesy of ReachOut.com

What does cyberbullying look like?
- Being sent mean or hurtful text messages from someone you know or even someone you don’t know.
- Getting nasty, threatening or hurtful messages through social networking sites like Facebook and Twitter, or through sites where people can ask/answer questions like Formspring or internet forums.
- People sending photos and videos of you to others to try and embarrass or hurt you.
- People spreading rumours about you via emails or social networking sites or text messages.
- People trying to stop you from communicating with others.
- People stealing your passwords or getting into your accounts and changing the information there.
- People setting up fake profiles pretending to be you, or posting messages or status updates from your accounts.

Cyberbullying – what it is and why it sucks

Cyberbullying is bullying that is done through the use of technology, for example, using the internet, a mobile phone or a camera to hurt or embarrass someone. It can be shared widely with a lot of people quickly, which is why it is so dangerous and hurtful.

Why is cyberbullying so bad?
- A lot of people can view or take part in it.
- It is often done in secret with the bully hiding who they are by creating false profiles or names, or sending anonymous messages.
- It is difficult to remove as it is shared online so it can be recorded and saved in different places.
- It is hard for the person being bullied to escape if they use technology often.
- The content (photos, texts, videos) can be shared with a lot of people.
- This content may also be easy to find by searching on a web browser like Google.

How to protect yourself
- Don’t share your private information like passwords, name and address, phone numbers with people you don’t know. Be cautious about sharing photos of yourself, your friends and your family.
- Don’t respond to messages when you are angry or hurt – either to strangers or people you know. This will often encourage them to continue or increase their harassment of you.
- Log out and stop messaging if you feel you are being harassed.
- Remember you have the option to block, delete and report anyone who is harassing you online and on your mobile.
- Find out how to report bullying and harassment on each of the different social networks that you use – see the Easy guide to socialising online on the reachout.com website for info on how to do this on different sites.
- Keep a record of calls, messages, posts and emails that may be hurtful or harmful to you.
- Remember to set up the privacy options on your social networking sites like Facebook in a way you are comfortable with.

For legal stuff, check out the Bullying and the Law fact sheet at reachout.com

The Australian Human Rights Commission (1300 656 419) has a complaint handling service that may investigate complaints of discrimination, harassment and bullying.

What CAN I DO NOW?
- Keep a record of what has been said and done online.
- Find out more about your legal rights when it comes to bullying.
- Talk to someone about what’s going on, whether that’s a teacher, parent or counsellor.

Signs this might be a problem ...
- People share embarrassing photos of you online.
- Harassing calls, texts or emails.
- People posting bad stuff about you online.
- People using your Facebook and Twitter to say humiliating stuff.
- People setting up fake profiles pretending to be you.

Cyberbullying and harassment can be difficult to deal with. The fact sheet advice reproduced courtesy of ReachOut.com is a good place to start.

What the experts say about cyberbullying

Professor Donna Cross offers advice on effective strategies for parents and schools, in this fact sheet from schoolatoz

AT A GLANCE

> Kids are more likely to refer to cyberbullying as texting, flaming, happy slapping, etc.
> Kids who may never bully face to face will do it online because it’s hidden.
> Even the kindest, most passive child can inadvertently contribute to cyberbullying by forwarding on a humiliating, abusive or confidential message.
> Spend time in your child’s online world to understand it.
> Kids won’t tell an adult about cyberbullying if they fear the result will be having their phone or internet access taken away.

While research into cyberbullying is still in its infancy, the one thing we do know is the online environment is really just a new setting for age-old issues.

Cyberbullying is an extension of face-to-face bullying. It’s all about relationships. So far, there haven’t been any Australian research findings released about effective solutions to cyberbullying – but it’s being studied. Professor Donna Cross from Edith Cowan University in Perth is looking at effective strategies for parents and schools.

Donna has also been heavily involved in much of the research schoolatoz has to date.

WHEN ARE KIDS MOST VULNERABLE TO BULLYING?

> The first peak coincides with children discovering the power of the peer group, and creating their own social pecking order.
> The second peak occurs when children move from primary school to secondary school. In NSW it’s in Year 7. In WA, where high school begins a year later, it’s in Year 8.
> This later peak is all about social groups being mucked up. The social hierarchies that were well established are now all in disarray as new kids are thrown together in a new school. Every time you change the group, you increase the likelihood of bullying.

WHO CYBERBULLIES?

> Although technology doesn’t cause bullying, it changes the nature of it. Kids who may never bully face to face will do it online because it’s hidden, can be anonymous and they don’t get feedback from the victim or peers of the harm they are causing.
> It’s also easier for misunderstandings to occur – and become inflamed – when using the written word. Again, there are none of the traditional cues we use with our face and voice to convey humour or sadness, etc.

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: St Mark’s Anglican Community School, Hillarys, libraryadmin@stmarks.wa.edu.au

Issues in Society | Volume 381

Online Safety 39
• The speed of online communication can contribute to bullying. Kids respond immediately without taking time to think through the consequences, or potential problems. (Who hasn’t sent an email in a hurry and realised it’s full of errors?)

• We also don’t have good definitions of cyberbullying yet. Some experts say it needs to be intentional, repeated and between two people with different levels of power. Some parents would argue that one incident between kids the same age is also cyberbullying.

• Even the kindest, most passive child can inadvertently contribute to cyberbullying by forwarding on a humiliating, abusive or confidential message.

WHAT PARENTS CAN DO TO STOP CYBERBULLYING

• Understand where your kids are going online, what they are doing, and who they are talking to – this is absolutely vital.

• Spend time in your child’s online world. You can’t understand it otherwise.

• Accept and acknowledge how important technology is to your child.

• Don’t ask your child if they’re being cyberbullied. Use their language – have they seen mean texts circulating, humiliating photos or messages on others’ Facebook walls?

• Don’t downplay covert bullying. Parents and teachers can sometimes say things like “don’t worry ... it doesn’t matter if you’ve been left out”, or “just ignore the bullying”. This tells the child that you don’t take their situation seriously, and can even convey the message it’s OK and normal for others to treat them this way.

• Kids won’t tell an adult about cyberbullying if they fear the result will be removal of the phone or internet access. Discuss this with your child and reassure them that’s not how you’ll deal with it.

• Teach your kids how to be good cybercitizens (careful, private, empathetic) before they reach Year 4 (by about nine years old, or when they may begin to venture online).

• Much of cyberbullying and face-to-face bullying is learned behaviour. Look at what behaviours you’re modelling to your kids. Is sarcasm and point-scoring part of your family culture? It’s often how you say something that matters.

• Don’t contact the other child, but do tell the school principal.

• Don’t immediately assume your child is being victimised and the other child is just a bully. Miscommunications get out of hand quickly and often both parties feel hurt.

This article is from www.schoolatoz.nsw.edu.au – helping parents with their child’s homework and wellbeing. Created by NSW Department of Education and Communities.

CYBERBULLYING AND YOUNG PEOPLE

When young people experience bullying behaviour online, it can be difficult to spot. To help your child, you can learn about cyberbullying – what it is, when to step in, and what to do about it. A guide from Raising Children Network

What is cyberbullying?

Cyberbullying (or online bullying) is using modern communication technology to deliberately and repeatedly harass, humiliate, embarrass, torment, threaten, pick on or intimidate someone.

Cyberbullying happens in lots of different ways – by mobile phone, text messages, email, or through social networking sites such as Facebook. Examples of cyberbullying include sending anonymous threatening emails, spreading rumours on the school e-bulletin board to break up friendships, or setting up an unkind or unpleasant fake social networking account using real photos and contact details.

Effects of cyberbullying

Cyberbullying can leave teenagers with low self-esteem, less interest in school and a deep sense of loneliness. Some feel they have no safe place, because the bullying can happen anywhere there’s internet or mobile access. It can also happen at any time of the day or night.

Nearly one quarter (23%) of children who use mobile phones have reported receiving a threatening or abusive text, and 14% reported sending one.

Helping your child avoid cyberbullies

You can help make cyberbullying less likely to happen to your child by:

- Discussing cyberbullying when your child first starts to use the internet or a mobile phone. Talk about what forms cyberbullying can take, the consequences it can have, and how it’s best to never pass along or reply to bullying material.

Cyberbullying happens in lots of different ways – by mobile phone, text messages, email, or through social networking sites such as Facebook.

- Talking with your child about online friends and messaging friend lists. Explain that adding someone your child doesn’t really know as a ‘buddy’ or ‘friend’ gives that person access to information about her that could be used for bullying.

- Teaching your child not to give out passwords to friends. Some teenagers do this as a sign of trust, but a password gives other people the power to pose as your child online.

- Teaching your child to ‘think before posting’. Young people who post personal information online (like suggestive photos or videos) can also attract unwanted attention, negative comments or ridicule. This kind of personal information might be available online for a long time, well after your child is comfortable with other people seeing it.

DID YOU KNOW?

- In a recent study, 20% of all the teenagers surveyed said they’d been cyberbullied.
- The problem was most common in girls – nearly 1 in 4 reported having been the victim of a cyberbully.

A recent study suggested that 20% of teenagers have engaged in cyberbullying behaviour at some point. There’s no denying that cyberbullying is harmful. But if 20% of teenagers have engaged in bullying or been bullied, that means that 80% are using the internet happily and responsibly.

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: St Mark’s Anglican Community School, Hillarys, libraryadmin@stmarks.wa.edu.au
How to spot cyberbullying

Cyberbullying can be tough
to spot. Many young people who
are being bullied don’t want to
tell teachers or parents, perhaps
because they feel ashamed or they
worry about losing their computer
privileges at home.

As a parent, you might find it
hard to keep up with the different
technologies your child uses. Or you
might not know how to bring up
the subject of cyberbullying.

Some warning signs that your
child might be the victim of cyber-
bullying include:
• Being upset during or after
using the internet
• Withdrawing from friends and
activities
• Being more moody than usual,
or showing obvious changes in
behaviour, sleep or appetite
• Spending much longer than
usual online, or refusing to use
the computer at all
• Exiting or clicking out of a
computer activity if a person
walks by
• Avoiding school or group
gatherings
• Bringing home lower marks
than usual
• ‘Acting out’ in anger at home
• Having trouble sleeping
• Feeling sick or complaining of
frequent headaches or stomach
aches.

Helping teens handle cyberbullying

If teenagers are being bullied
online, it’s great for them to feel
they have some power to resolve the
problem on their own.

Examples of cyberbullying
include sending
anonymous threatening
emails, spreading rumours
on the school e-bulletin
board to break up
friendships, or setting up
an unkind or unpleasant
fake social networking
account using real photos
and contact details.

These six steps are a good way
for your child to G.E.T. R.I.D.
of the bully:

1. Go block or delete the person
engaging in cyberbullying.

Blocking from friend lists helps
stop the person engaging in
cyberbullying from posting or
uploading offensive content
about your child. If it’s a text
message or call, you can call the
service provider and have the
calls/texts monitored. If neces-
sary, the service provider can
even contact the sender, since

Worried your child might be the
one doing the bullying? For ideas
on encouraging your child to treat
other people with respect online,
you could read the article on being
a responsible cybercitizen on the
Raising Children Network website.

GLOSSARY

Facebook
A website that allows users to build an online profile with personal details,
photos, videos and other information. Users can add friends, send them
messages, and let friends know what they are doing via ‘status updates’.
Users can also comment on their friends’ status updates, photos and videos.
These activities are called social networking.

Friend list
A list of people who have access to your profile – or different parts of your
profile – on a social networking site such as Facebook. When using social
networking sites, it’s important to think about whether you want all your friends
to see all your personal information. Sometimes, friends of your friends might be
able to see your information too. You can use friend lists to organise friends into
different lists, and customise privacy settings for different friend lists.
mobile phone holders breech their contract if they use their phone to bully. If necessary, you can change the phone number.

2. Ensure you keep evidence of bullying. Save and print out any bullying messages (use the print screen key, at the top right of most keyboards).

3. Tell someone. Sharing feelings with a parent, older sibling, relative, teacher or close friend will help keep your child from feeling isolated.

4. Report abuse. Reporting bullying to web administrators is usually as easy as clicking on a 'report abuse' link on a website. The website will remove the offensive content. There could also be consequences for the person engaging in bullying. If your child has been threatened, he should also report it to the local police.

5. Ignore bullying behaviour. This means not responding aggressively to taunts. It’s OK for your child to tell the person engaging in bullying to stop, but they shouldn’t try to fight fire with fire.

6. Delete the bullying message (after saving a copy), and don’t forward via text or send chat logs to others.

You might like to check out the illustrated guide to stopping cyberbullying on the Raising Children Network website. It’s a handy reference that you could print out for both you and your child to use.

Helping teens who have been cyberbullied
Your child won’t always be able to solve cyberbullying problems independently. It’s always worth stepping in if you’re concerned about her, as you’ll be able to help practically and emotionally.

Loving support is vital. Also:
• Talk to your child – listen to his side of the story, and reassure him that the bullying isn’t his fault.
• Let your child know that you’ll help and that things will get better.
• Stay calm and resist the temptation to ban the internet in your home. Banning online activities will only make your child less likely to share her online problems.
• Speak with the school if the problem involves a classmate. It’s best to make sure your child knows about your interaction with the school, and that he has a say in the process.

How cyberbullying is different from other bullying
Cyberbullying is different from other kinds of bullying, for both the person engaging in bullying and the victim. People using bullying behaviour will often act more boldly online than if they were facing their victim in person. Sending taunts remotely and anonymously makes the person doing the bullying feel safer. The victim’s physical or emotional response, which might change or soften the bullying behaviour, can’t be seen.

For the person being bullied, cyberbullying is tough to deal with. Because teenagers use mobiles and the internet so often, bullying can happen at any time, not just when they’re at school. The victim might not know who’s doing the bullying or when the bully will strike next. This can make teenagers feel persecuted and unsafe, even at home.

Bullying messages posted online are very hard to get rid of. These messages can be forwarded instantly and seen by many people, instead of just a few kids in the schoolyard.

ACKNOWLEDGEMENTS
Article developed in collaboration with Tena Davies, psychologist.

Sourced from the Raising Children Network’s comprehensive and quality-assured Australian parents website, http://raisingchildren.net.au

The recent arrest by Canadian police of two young people who allegedly shared a photo of a young woman being sexually assaulted has once again highlighted the danger that social media can pose for teenagers. The 17-year-old girl was bullied after the photo, which was taken in 2011, went viral. She died a few days after a suicide attempt in April.

Canadian police initially failed to lay any charges despite a year-long investigation. But the case has caused such outrage that Nova Scotia, the province where it took place, has introduced a law allowing people being bullied online or their parents to sue the perpetrator.

This kind of case is becoming more common with the proliferation of social media and Australia is in the enviable position of not having had a case of cyberbullying leading to death.

And there are things we can do to ensure we don’t have to.

A new landscape

A regulatory response would show that the law applies equally to behaviour online, but cyberbullying and suicide are complex individual and social issues that require a complex multi-faceted response.

We know that young people are uniquely vulnerable to bullying – as both victims and perpetrators, both online and off. They’re acutely sensitive to peer appraisal and rejection, and are also more prone to do thoughtless and cruel things when spurred on by their peers.

Bullying has always had negative consequences, but the all-pervasive reach of the online world magnifies its impact. Social media is accessible to everyone all the time. And a smart phone is the permanent accessory of the teen – constantly available to record, receive and respond to text messages and images.

Privacy has changed forever and there’s little respite for today’s teenagers. They face a relentless need to manage their online social identity and reputation, and the ever-present possibility of public humiliation.

How to help kids

Our first response should be to support teenagers to be informed and empowered users of social media, as well as responsible online social citizens.

Useful resources are increasingly available, but this education is too important to be ad hoc. We need to build it into routine learning at school.

Knowing how and where to seek appropriate help when they are distressed and feeling vulnerable is also critical for young people.

We know that teenagers don’t think through the consequences of their actions in the same way that adults do. This means we can’t expect young people to always monitor and moderate their own behaviour without help.

Adults have a duty to protect young people when they are vulnerable, and this duty increases in inverse proportion to the child’s age.

How to help the grown-ups

We also need to ensure that parents (and other adults responsible for young people) are well-informed about online safety, and know how to deal with bullying and where to seek help.

Parents must realise that effective monitoring of online behaviour is now part of their role, and they need to be vigilant about both bullying and victimisation.

The responsibilities of social media companies comprise another part of an effective response.

Facebook has rules regarding inappropriate content and processes for removing it. But these rely on the content being highlighted as such and judged to violate community standards.

And Twitter is initiating easier abuse notification. But as new social media products appear on the internet, there is no guarantee that they will have a sense of social responsibility.

Some new ways to share images and other content claim to increase user control (such as Snapchat where the amount of time an image is available can be limited), but this doesn’t preclude them from being used as avenues of bullying and abuse.

We could possibly do more with automated trawling to monitor content for keywords that indicate risk, and raise the alarm – potentially even to parents.

It will take time to find effective ways to monitor and moderate online environments – through the technology of the platforms themselves, and the engagement of parents and others in the community, including the police when necessary.

Social media is now a part of our social fabric and we all have a role to play to help keep young people safe from its darker side. Social media companies need to renew their efforts and it may well be time to start talking about the kind of regulatory measures we can take as a nation to help reinforce positive social norms.

Debra Rickwood is Professor of Psychology at the University of Canberra.
Can a cyberbullying commissioner protect our kids?

A federal government discussion paper has proposed the creation of a children's e-safety commissioner to help protect children from cyberbullying on social media. However not everyone agrees on the proposal, which opponents say is a slippery slope to government censorship, writes ABC Radio National’s Damien Carrick

Cassie Whitehill knows only too well the harm that can be caused by cyberbullying. Last year her sister Chloe, age 15, ended her life after ongoing physical and cyberbullying. The last straw for Chloe was being attacked on a Hobart street and then being told that a video of the assault would soon be posted on Facebook.

Whitehill says although this footage was never posted, cyberbullying over a long period of time played a corrosive role in her sister's life.

"Name-calling, threatening, saying that she was going to get smashed, things like that ... We had reported a couple of posts on Facebook, and they'd as usual come back saying that it doesn't breach their community standards."

Name-calling, threatening, saying that she was going to get smashed, things like that ... We had reported a couple of posts on Facebook, and they’d as usual come back saying that it doesn’t breach their community standards.

Facebook declined to comment on Chloe’s case.

In January the federal government released a discussion paper titled Enhancing Online Safety. It canvasses a number of proposals which would tighten regulation in the online space.

Paul Fletcher, the parliamentary secretary for communications, says that the large social media sites generally have complaint reporting mechanisms and clear terms of use.

"If you lodge a complaint, in some cases you don’t even know whether it’s been received or not, but more substantively it’s essentially a matter for the discretion of the site as to whether the site chooses to take action and remove the material or not,” he says.

The government is proposing to create a children’s e-safety commissioner with the power to demand social media sites rapidly remove material that is harmful to a child.

"What we’re proposing is that the first step would be to use the existing complaints scheme of the large social media site, but that if you get no response there you would then be in a position to go to the commissioner. The commissioner would then apply a statutory test. Now, the test that we’ve proposed as the indicator of cyberbullying is content targeted at and likely to cause harm to an Australian child.”

Last week the digital industry association AIMIA, together with some of the big online big players like Microsoft, Facebook, Google, eBay and Twitter, released a joint press release highly critical of the proposal.

“The government’s proposal to legislate a one-size-fits-all regime is counterproductive to our own work and commitment to the safety of people who use our services,” the release announced. “Also the creation of a new statutory body and a new regulation on complaints handling seems to be at odds with the government’s stated strategy to reduce regulation and to streamline government agencies.”

However, Fletcher rejects the criticism, and says the new regulation will not be a burden to businesses or individuals.

“We have been quite careful in limiting the reach of the measures that we are proposing here. There has been some commentary about impacts on free speech, for example, but we have quite carefully limited this. First of all, it applies only to communications directed at children. So it’s a specific measure designed to protect children. It has no impact on speech between adults.”

Jon Lawrence, executive officer of Electronic Frontiers Australia, is not convinced.

“It sounds to us a little bit like a fairly standard procedure for a new government to be seen to be doing something about a problem,” Lawrence says.
“It’s not clear to us that creating any new legislation or any new bureaucracy is really going to be helpful in this context.”

“I think those social media platforms that have a presence here in Australia on the whole are actually pretty proactive in dealing with these issues. They are engaged with government on the whole ... and I think in the case of particularly Google, Facebook and YouTube they are reacting pretty quickly to a lot of these issues.”

The government is proposing to create a children’s e-safety commissioner with the power to demand social media sites rapidly remove material that is harmful to a child.

Lawrence is also concerned that pulling down material likely to cause harm is too broad a category.

“It’s very hard to define. You could have a very simple thing of somebody calling somebody else fat, which for some kids could be really hurtful, for others maybe not so much ... When you have very broad and subjective definitions like that, the potential for it to sort of creep into what could potentially actually be a government sponsored censorship program I think is not unlikely.”

Not surprisingly, Cassie Whitehill takes the opposite view and says she would welcome any regulation.

“If you or someone you know is experiencing a crisis, you can call Lifeline on 13 11 14.

The discussion paper Enhancing Online Safety for Children is available from www.communications.gov.au

Reproduced by permission of the Australian Broadcasting Corporation and ABC Online. © 2013 ABC. All rights reserved.

As many as one in three Australian children has experienced some form of cyberbullying, yet the system to control bad behaviour on social media networks is voluntary, with the industry largely self-regulated. Tracey Bowden reports for ABC News

The Federal Government has released a discussion paper proposing a number of changes to help make children safer online, but critics of the proposal say another layer of bureaucracy is not the answer.

Cristina Asarloglou sobs as she talks about her daughter Anastasia, who is among the thousands of Australian children who have experienced bullying online.

“She said to me that she didn’t want to live anymore and I couldn’t believe a child at eight years old could say that she didn’t want to live anymore,” Ms Asarloglou said.

“Bullying has always existed, but now with online bullying it just intensifies it.

“Anything to help kids that are being affected by this is something because I believe it is an epidemic.”

For some children the relentless bullying becomes too much. Chloe Fergusson took her own life six months ago at the age of 15. Her sister Cassie Whitehill is calling for tougher bullying laws and enforceable take down orders, and has set up a website promoting what she calls “Chloe’s Law”.

“If we can just save one young person from taking their own life or being affected by bullying then we’ve achieved our goal,” she said.

Cybersafety consultant says voluntary system not working

Cybersafety consultant Alastair MacGibbon says the current system in Australia, where the removal of damaging material from social media sites is voluntary, is not working.

“You talk to parents who ask ‘what can I do if I have been going to providers and nothing gets done, who can I turn to?’ And there is no answer for them at the moment,” he said.

The Government hopes to provide an answer, and has received almost 100 submissions in response to its discussion paper on children’s e-safety. The measures announced include the establishment of an e-safety commissioner, with the power to have harmful material removed quickly.

“This scheme would be backed by legislation and so it would apply to large social media sites,” said Parliamentary Secretary for Communications Paul Fletcher.

“As with any legislation there would be an obligation to comply with the requirements and a failure to comply would carry some sanctions.”

Mr MacGibbon supports the idea of some form of penalty.

“I think a civil regime of penalties where offenders who put content online can be fined, if they don’t take that content down, and service providers who don’t do the right thing ... can equally be fined as well, is a good thing,” he said.

But not everyone welcomes the Government’s proposals.

David Holmes from the Australian Interactive Media Industry Association (AIMIA), which represents social media networks like Google and Facebook, says under the current system, companies can remove bullying material within 24 to 48 hours.

“We don’t disagree with the purpose of what we are trying to achieve, which is to make that take down faster. We just don’t believe legislation is the way to do it,” he said.

He says another layer of bureaucracy will not help.

“The big guys that this proposed legislation is looking at really are leading the way globally, it is in their interest to look after their members online,” he said.

“So they are well and truly making sure that the bullies get eradicated.”

But Mr MacGibbon disagrees.

“If the regime for notification and take down is working, then there is no burden at all having an e-safety commissioner for children,” he said.

“If, however, as many of us suspect, there are complaints being made to these social networking sites and either no action or the wrong action is being taken, then it might well be a burden to them and I would suspect the average Australian would say ‘good, put a burden on them.’”

Reproduced by permission of the Australian Broadcasting Corporation and ABC Online. © 2013 ABC. All rights reserved.
Trolling and flaming refer to the intentional disruption of online communities. While closely related, the general difference is that trolling is considered to be rude or impolite commentary and posts, lacking in etiquette, while flaming refers to insulting or provocative commentary (Hardaker 2010; Herring et al. 2002). An information sheet from the Australian Institute of Criminology here is a lack of clarity concerning the definition of trolling. For example, senders may not have intended to troll (i.e. to be rude or impolite); instead, they may have misunderstood the context of the discussion, or made an error that has been misinterpreted (Hardaker 2010). The exchange may then escalate when others add their opinions. In contrast, motivations for flaming included passing time, escaping from reality, relaxation and entertainment (Alonzo & Aiken 2004).

Trolling and flaming may be opportunistic, or specifically directed at individuals or groups, particularly those who are already discriminated against (Herring et al. 2002). Trolling and flaming are facilitated by the perceived anonymity and physical distance between the troll and the victim, and they typically take place on social media sites, blogs and online discussion forums (Hardaker 2010; Herring et al. 2002).

Trolling and flaming, when persistently directed at the same target(s), may constitute cyberstalking or cyberbullying and the effects on the intended victim may be similar, including feelings of anger, powerlessness, sadness and fear (Hoff & Mitchell 2009).

The Australian Communications and Media Authority (2004) has provided the following advice to protect against trolling and flaming:

- **IGNORE** the troll – don’t respond to nasty, immature or offensive comments. Giving trolls the attention they want only gives them more power.
- **BLOCK** the troll – take away their power by blocking them. If they pop up under a different name, block them again.
- **REPORT** trolls – report to site administrators. If they pop up under a different name, report them to site administrators again. If they continue, contact the police for further advice.
- **TALK** with friends and family – if a troll has upset you, talk about it with friends and family – it’s not you, it’s them. Visit the Cybersmart Online Helpline or call Kids Helpline on 1800 55 1800 (or LifeLine on 13 11 14).
- **PROTECT** friends from trolls – if trolls are upsetting a friend tell them to Ignore, Block and Report. Tell their family and other friends and encourage them to seek support.

Evidence of trolling or flaming may be obtained by taking screenshots or printing the offending pages. Where there is a threat to safety, trolling and flaming should be reported to the police. Civil action may be an option where defamation has occurred.

### NEED TO KNOW MORE?

Stop the trolls: how to prevent cyberstalking happening to you

Online stalking gets far too much attention, but it’s worth making some changes to prevent it happening to you, cautions Rosemary Purcell

Recent cases of online abuse against Charlotte Dawson and NRL player Robbie Farah have attracted considerable media attention and triggered public debate about how to respond to this issue.

But how big a problem is online abuse and harassment, and is it serious enough to warrant this level of attention and concern?

Not according to current research, but prevalence studies are thin. For example cyberstalking, which involves repeated, unwanted contacts via the internet, email and other communication technologies, is relatively uncommon. Only 5-10% of stalking victims report having been cyberstalked. Instead, most stalking occurs offline, where victims are followed, kept under surveillance, intruded upon at home or work, and harassed via phone calls.

A WEALTH OF OPPORTUNITY

The concern about online abuse appears to be driven more by the potential, rather than actual size of the problem. More than half a billion people worldwide share information every day about their lives on Facebook alone, let alone other social media platforms such as Twitter or LinkedIn. The scope for abuse is immense, whether via isolated instances of inflammatory and offensive postings (‘trolling’) or more relentless campaigns of cyberbullying or stalking.

The very nature of cyber abuse or stalking may promote the behaviour, as it’s pursued in private and often with anonymity (although as the recent ‘trolling’ cases demonstrate, beliefs in anonymity may be misplaced). In online environments that lack an obvious social context, or rules or norms that might otherwise inhibit deviant behaviour, online abuse and harassment may appear ‘unaccountable’ to some individuals and therefore more feasible.

That said, in the non-cyber world, many people abuse, bully, harass or stalk others regardless of social and moral conventions.

More research is needed to understand the nature and prevalence of all forms of online abuse. But online services that are designed to help victims of online abuse
Online abuse in all its guises is a serious form of violence. The most common forms of cyberstalking include publishing potentially damaging or embarrassing personal information online or via email, spreading false or malicious rumours about the victim and gathering information about a victim.

ONLINE IS STILL REAL

Issues of prevalence aside, online abuse in all its guises is a serious form of violence. The most common forms of cyberstalking include publishing potentially damaging or embarrassing personal information online or via email, spreading false or malicious rumours about the victim and gathering information about a victim (their home address, phone number, photos of friends or relatives and so on).

The sense of violation caused by these acts is damage enough to the victim and likely to be amplified when the abuse is shared widely via social media. Research clearly indicates that cyberstalking does not differ from its physical world counterpart in terms of the impact on victims.

Victims of both can suffer emotional damage, including profound feelings of mistrust, helplessness, depression, anger and even paranoia, as they live in anticipation of the next potential invasion of privacy or abusive contact.

JUST SWITCH OFF?

That’s often helpful in the short term, if only to ‘re-group’ and remove yourself from the abuse. What’s more critical in these situations is self-control. People who are subjected to online abuse, harassment or stalking should avoid any further contact or confrontation with the perpetrator. These people thrive on attention and any reply or response to the abuse is almost guaranteed to be met with ‘more of the same’. Restraint is easier said than done. But this strategy is one of the most effective ways of bringing harassment and stalking to an end.

In addition, most Australian states and territories have laws that could be used as a legal remedy to address these forms of online abuse.

A NEW WORLD ORDER ...

The explosion in the use of social media and a relaxation in inhibitions about sharing personal information online have presented challenges and made mindfulness about practical protections more relevant.

Critical strategies to enhance safety online include:

• Being continually vigilant about the privacy settings on social media accounts. This is often not a straightforward process of merely ticking a box (Facebook, for example has more than 100 privacy setting combinations).
• Consider deactivating ‘Location Settings’, as this can allow anyone to know your real time locations, and lead them there via Google maps.
• Resist the urge to regularly ‘check-in’ as this gives an insight into your daily habits.
• Be aware that new features such as Facebook’s ‘Timeline’ allows people to trawl back through your entire online history, including the days when we were all a little less social media savvy.
• Google yourself, and if any information that you regard as private is revealed, contact the website administrator and have them remove the details.
• Ask friends, family and acquaintances not to post any information about you that you regard as personal and private, including your contact details or photos.
• Don’t disclose anything online that you wouldn’t feel comfortable telling a stranger offline.

Rosemary Purcell is Associate Professor at the University of Melbourne.

PERSONALITY DIFFERENCES: TROLLS AND CYBERSTALKERS AREN’T THE SAME

Lumping trolling in with cyberstalking obscures the very different reasons that people have for behaving badly online, and the different responses that might be needed, writes Troy McEwan.

The recent death of television personality Charlotte Dawson and the possible role that online abuse played in her struggles with depression shows how damaging this behaviour can be.

The former model had told of her battles with depression and the abuse and harassment she suffered from users of social media website Twitter. Since Dawson’s death on the weekend, experts have pointed out that existing stalking laws could be used to respond to those who abuse people online.

Despite their legal similarities, new research is shedding light on the personality differences between online ‘trolls’ and stalkers.

Trolls and stalkers

It seems like online abuse is now so common that any offensive or potentially harmful comment posted on social media is called ‘trolling’.

The problem is, online abuse can range from one-off racist, sexist or otherwise distasteful comments to threats of rape and violence and sustained campaigns of harassment that cause significant psychological harm.

Lumping trolling in with cyberstalking obscures the very different reasons that people have for behaving badly online, and the different responses that might be needed.

How to best respond to a hateful or threatening comment probably depends on who is sending it to you and what they are trying to get out of it.

The terms trolling and cyberstalking do overlap as both involve repeated, online and harmful actions.

In academic literature, trolling is acting in deceptive, disruptive and destructive ways in internet social settings with no apparent purpose. Cyberstalking is using the internet to repeatedly target a specific person in a way that causes them distress or fear (reflecting descriptions of offline stalking).

Using these definitions, some trolls could be considered cyberstalkers, and vice versa. But new evidence on trolling suggests that the actions of a troll might meet different psychological needs to those of a cyberstalker.

The personality of a troll

Researchers from Winnipeg conducted a study earlier this month on the personality characteristics of internet trolls.

Online abuse can range from one-off racist, sexist or otherwise distasteful comments to threats of rape and violence and sustained campaigns of harassment that cause significant psychological harm.

In particular, they explored whether trolls reported the personality traits of:

- **Machiavellianism** – willingness to manipulate and deceive others
- **Narcissism** – grandiosity and entitlement
- **Psychopathy** – lacking remorse and empathy
- **Sadism** – taking pleasure in the suffering of others.

They found clear evidence that trolling is associated specifically with self-acknowledged sadism (and to a lesser degree with Machiavellianism).

What’s more, people who reported sadism tended to troll because they
found it to be pleasurable. As the researchers concluded: “Sadists just want to have fun ... and the internet is their playground!”

The trouble with stalkers
The results of this interesting study are remarkably different to what we know about cyberstalkers (and stalkers more generally):

1. Unlike trolling, there is a high degree of overlap between online and offline stalking, with 70% to 80% of cyberstalkers using both behaviours.

2. There is no evidence to suggest that cyberstalkers are motivated by sadism, though personality disorders involving poor emotional control and antisocial attitudes are reasonably common in this population.

Research suggests that, rather than primarily taking pleasure in their behaviour, stalkers (including cyberstalkers) are more likely to be highly distressed and angry with the victim. While they may get secondary pleasure from it, stalkers who intimidate or threaten usually have the very specific purpose of expressing their negative feelings and making the victim feel as bad as they do.

How to respond
So if trolling and cyberstalking occur for different psychological reasons, does that mean that different responses are required for each? From the research to date, the answer is yes.

It seems like trolls are in it for the ‘fun’ of provoking a response, whereas cyberstalkers are more emotionally invested in pursuing the victim. This raises the possibility that the advice “do not feed the trolls” may have genuine support.

When the troll fails to provoke a response, he or she may look elsewhere for their fun, at least on that particular occasion.

In the longer term, if trolling is meeting a sadistic need as the Canadian researchers suggest, it’s probably safe to assume that they’re going to keep doing it – just not necessarily to the same person.

On the other hand, ignoring the cyberstalker may have the opposite effect. Like the troll, the stalker is after a response, but unlike the troll, they need a response from this victim.

They can’t just move on to another person because the issue that led to the stalking is victim-specific. Totally ignoring cyberstalking may not only inflame the stalker’s emotions, but lead to an escalation in behaviour.

An immediate online response isn’t advisable (it can be equally enraging for a stalker), but a cyberstalker will likely require some sort of response to stop the harassment.

Before a target chooses a response, they should think about who is harassing them and why they might be doing it.

If they think they have a prior relationship with them (of any sort), if they are using multiple different methods to harass the person, or if it has gone on for more than a week or so, they may be dealing with a cyberstalker.

If so, they may need to start recording evidence and consider whether or not to involve the police. If this is a one-off, provocative contact from an unknown person, it may be a troll looking to provoke and the best thing to do is ignore it.

Trolls should be reported to the website host and in any situation where there an explicit threat or where a person feels scared by the behaviour, the most appropriate thing to do is to save the evidence (take a screenshot and print it) and take it to the police.

People can also consult websites such as Cybersmart, Wired Safety, Cyberangels and Halt Abuse, or the US Stalking Resource Centre.

Troy McEwan is a lecturer in Clinical and Forensic Psychology at Swinburne University of Technology.

Lumping trolling in with cyberstalking obscures the very different reasons that people have for behaving badly online, and the different responses that might be needed.
WORKSHEETS AND ACTIVITIES

The Exploring Issues section comprises a range of ready-to-use worksheets featuring activities which relate to facts and views raised in this book.

The exercises presented in these worksheets are suitable for use by students at middle secondary school level and beyond. Some of the activities may be explored either individually or as a group.

As the information in this book is compiled from a number of different sources, readers are prompted to consider the origin of the text and to critically evaluate the questions presented.

Is the information cited from a primary or secondary source? Are you being presented with facts or opinions?

Is there any evidence of a particular bias or agenda? What are your own views after having explored the issues?

CONTENTS

BRAINSTORM 54
WRITTEN ACTIVITIES 55
MULTIPLE CHOICE 56
Brainstorm, individually or as a group, to find out what you know about online safety.

1. What is cyberbullying, and why is it an issue?

2. What is cyberstalking, and who does it affect?

3. What is sexting, and what are the risks and consequences?

4. Explain the difference between trolling and flaming.
Complete the following activity on a separate sheet of paper if more space is required.

It is important to understand how personal information is used online and how you can manage and protect your information and digital reputation.

List at least four (4) ways you can secure your personal information and digital reputation when registering for, and participating in, the following online activities:

SOCIAL MEDIA (FACEBOOK, TWITTER, ETC)

PICTURE / VIDEO MESSAGING SERVICES (SKYPE, SNAPCHAT, ETC)

SUBSCRIPTIONS / COMPETITIONS

GAMING
Complete the following multiple choice questionnaire by circling or matching your preferred responses. The answers are at the end of this page.

1. Which of the following would be the safest password for online use?
   a. janesmith1999
   b. jane1234
   c. 1111janesmith
   d. j@ne^5x2
   e. janesmith

2. Which of the following are indicators your mobile phone or device may have been attacked by malicious software? (Select all that apply)
   a. There are messages in your sent folder that you never sent
   b. You are suddenly receiving lots of advertising on your phone
   c. The user interface has changed without you taking any action to change it
   d. Large amounts of money suddenly appears in your bank account
   e. A sudden increase in your phone bill with no obvious reason
   f. You receive free gifts in the post

3. What should you do if you receive an email from someone you don’t know with a generic subject line and an attachment?
   a. Open the email to see what it’s about
   b. Save the email
   c. Open the attachment as it may be important
   d. Delete the email
   e. Reply to the email to ask them who they are

4. What should you do if you receive a request from someone you have never met to video chat?
   a. Connect straight away to see what they want
   b. Start up a messaging conversation with them
   c. Call the police
   d. Block the person
   e. Ignore the request

5. Match the following terms to their correct definitions.
   1. Phishing a. A message offering an attractive job vacancy with high pay and limited work, often involving transfers of money between accounts.
   2. Advance fee b. Any unwanted message sent to an email account or mobile phone.
   3. Lottery c. A message claiming that the recipient has won a substantial prize and asks for a fee to claim the prize.
   4. Mule d. Messages sent from a fake email address. These often claim to be from well known financial institutions or telecommunications providers and attempt to access the recipient’s financial and personal information.
   5. Spam e. A message that offers to pay a considerable amount of money to assist in transferring millions of dollars out of a foreign country, often with legitimate sounding reasons.

MULTIPLE CHOICE ANSWERS
a – d; b – a, b, c, e; c – d; d – a, b, c, e; e – a, b, c, e.
As part of their privacy policies, social networking sites such as Facebook, Twitter and YouTube specify that users must be at least 13 years old (AIFS, Online safety). (p.2)

Australian children are among the youngest and prolific users of the internet in the world (QUT, Aussie kids ‘earliest internet users’). (p.6)

76% of Australian children and young teenagers go online daily, with the average time spent online bordering over 1.5 hours per day (ibid). (p.6)

30% of Australian children reported encountering something online that upset or bothered them – 2.5 times the European average (ibid). (p.6)

Many young people fear that parents might take away their devices and refuse access to the internet and so do not report cyberbullying to their parents (ACMA, cyber[smart:] Parents’ guide to online safety). (p.7)

Some social networking sites, such as Club Penguin, are created especially for children under 13 years (ibid). (p.8)

Information posted online can be difficult or impossible to remove. An inappropriate image posted today can have a long-term impact on your digital reputation (ibid). (p.8)

Children can benefit from the internet because it offers them more text-based information than other media. This can help improve a child’s reading and problem-solving skills (Raising Children Network, Internet safety). (p.11)

Experts recommend limiting children’s daily screen time (including TV, DVD and computer). Current Australian guidelines are no more than 1 hour a day for children aged 2-5 years, and no more than 2 hours a day for children over 5 (ibid). (p.11)

Some content that is considered inappropriate may also be prohibited or illegal in Australia. Prohibited content is defined with reference to the National Classification Code categories RC, X18+, R18+ and MA15+ (ACMA, Offensive or illegal content). (pp. 14-15)

Facebook and Twitter give you the option of downloading a copy of all the information you have on your profile including photos, comments and your wall posts (AFP, Social Media Reputation Management). (p.18)

Bluetooth creates a wireless network between paired devices within a limited range. There are ways in which vulnerabilities in Bluetooth can be exploited, providing access to your address book, calendar, messages, photos and other content on your mobile phone (ibid). (p.18)

Under the Spam Act 2003 it is illegal to send or cause to be sent unsolicited commercial electronic messages in Australia (ACMA, Protecting personal information). (p.19)

Information posted and shared on social networking sites may be permanently recorded and users may not have control over who sees or accesses their personal information (ibid). (p.21)

Research shows that in America 97% of all children play video games and 2% are addicted (Splarm, H, How to help kids who are hooked on online gaming). (p.27)

Wagering and sports betting is legal in Australia. Australians can bet at offshore casinos however it’s illegal to provide online casino facilities from Australia (Turning Point, Online Gambling. So easy to bet. Too easy to lose). (p.30)

Illegal and offensive online content is regulated through the Online Content Scheme under Schedule 5 and 7 of the Broadcasting Services Act 1992 through a complaints-based mechanism (ACMA, Online content regulation). (p.31)

The ACMA can investigate a range of online content, including offensive imagery of children, material that advocates the doing of terrorist acts, content that incites, instructs or promotes in matters of crime or violence, as well as sexually explicit material (ACMA, Online content complaints). (p.32)

Studies show that over 95% of young Australians use the internet regularly (Department of Communications, Enhancing Online Safety for Children). (p.33)

Many 10-12 year olds use the internet from 1-3 hours per day. By 13, social media use has become the norm; and by 15, the internet and its use has become an ‘organic integrated part’ of everyday life. (ibid). (p.33)

In 2011, the use of social media was identified as the primary form of digital communication between young people over 13, overtaking more traditional digital means such as text messages, phone calls and email (ibid). (p.34)

The small minority of 12-17 year olds that do not have a Facebook account feel that they suffer a degree of social isolation and exclusion (ibid). (p.34)

53% of children own or access their first internet-connected device before 10 years old (ibid). (p.34)

The ACMA research indicates 4% of 8-9 year olds; 21% of 14-15 year olds; and 16% of 16-17 year olds reported being cyberbullied (ibid). (p.34)

Each day in Australia 100,000 children report they are bullied at lunchtime or recess. While that number includes all kinds of bullying, 80% of the children who are cyberbullied are also face-to-face bullied (NSW DEC, What the experts say about cyberbullying). (p.39)

23% of children who use mobile phones have reported receiving a threatening or abusive text, and 14% reported sending one (Raising Children Network, Cyberbullying). (p.41)

More than half a billion people worldwide share information every day about their lives on Facebook alone, let alone other social media platforms such as Twitter or LinkedIn (Purcell, R, Stop the trolls: how to prevent cyberstalking happening to you). (p.49)

Online abuse can range from one-off racist, sexist or otherwise distasteful comments to threats of rape and violence and sustained campaigns of harassment (McEwan, T, Personality differences: trolls and cyberstalkers aren’t the same). (p.51)

There is a high degree of overlap between online and offline stalking, with 70% to 80% of cyberstalkers using both behaviours (ibid). (p.52)
Online Safety

Cybersafety
Also referred to as ‘online safety’, ‘internet safety’, ‘e-safety’ or ‘digital safety’. It is defined as the safe and responsible use of information and communication technologies. Effective cybersafety strategies embrace and promote digital inclusion, digital literacy, digital citizenship and digital resilience. Cybersafety addresses a wide range of issues including:

- Online privacy (including the use of privacy settings)
- Online etiquette (or ‘netiquette’)
- Cyberbullying
- Sexting and ‘sextortion’
- Online sexual predation and grooming
- Personal information security
- Digital footprints (also known as ‘online reputation’)
- Safe social networking
- Accessing inappropriate content
- Internet and device addiction
- Safety when gaming online
- Security tools and filtering software
- Digital fraud
- Hacking
- Online piracy, and
- Plagiarism.

Digital media literacy
Comprises the technical and intellectual skills to access, understand, and participate in or create content on digital media and communications technologies. Well-developed digital media literacy enables users to make informed choices online. Digital literacy influences users’ ability to engage safely online because it guides decision making, interactions and interpretation of online information. There are three kinds of literacy required in a social media environment:

- Technical literacy – being able to successfully navigate technologies with technical skills
- Media literacy – understanding the opportunities new technologies can open up; working knowledge of available platforms; capacity to make judgements about the quality and reliability of online sources, and
- Social literacy – an understanding of the social norms that apply in online settings.

Digital citizenship
Describes the skills, knowledge, and values required to be an effective, ethical and safe user of information and communication technologies. Digital citizenship marks a shift to thinking about online practices as fundamentally social and community-based practices, as opposed to purely individual ones.

There are five elements of digital citizenship:

- Participation or ‘civic engagement’
- Literacies (digital, media, social)
- Rights and responsibilities
- Norms of behaviour (appropriate and responsible online behaviour or ‘good citizenship’)
- Sense of belonging (membership/connection with others).

Digital resilience
The ability to deal with negative experiences online or offline. Strategies focus on skilling users to adapt and respond effectively to potentially harmful online experiences. Cybersafety has conventionally focused extensively on extrinsic/external protections, such as parental monitoring, rules, laws, parental control technologies, law enforcement, etc., whereas digital resilience emphasises a more strengths-based approach, which focuses on intrinsic/internal protections, such as self-regulation and social literacy.

Grooming
Online grooming is the illegal act of adults making contact with a child online for the purpose of establishing a sexual relationship. Often this will be via a social networking site, but it may also be through other online services.

Mobile phone safety
Risks can include high or unexpected bill costs, cyberbullying, sexting, broadcasting their location to unintended others through ‘checking in’ and access to inappropriate material.

Offensive or illegal content
Offensive or illegal content may include topics, images or other information that are prohibited in Australia or could be damaging to young people online. This is content that may:

- Include footage of real or simulated violence, criminal activity or accidents, promote extreme political or religious views or be sexually explicit and can include illegal images of child sexual Abuse
- Promote hate towards individuals or groups on the basis of race, religion, sexual preference or other social/cultural factors, instruct or promote crime, violence or unsafe behaviour, like bomb or weapon making, anorexia, drug use, gaining unauthorised access to computers, fraud or terrorist activities.

Prohibited online content
Some content that is considered inappropriate may also be prohibited or illegal in Australia. Prohibited content is defined with reference to the National Classification Code categories RC, X18+, R18+ and MA15+.

Sexting
Sexting is the sending of provocative or sexual photos, messages, or videos, generally using a mobile phone or webcam. It can also include posting this type of material online. Young people often consider sexting as a way of connecting in a relationship.
WEB LINKS

Websites with further information on the topic
Australian Communications and Media Authority (ACMA)  www.acma.gov.au
Bullying. No Way!  http://bullyingnoway.gov.au
Communications Alliance  www.commsalliance.com.au
Cybersafety Help  www.cybersafetyhelp.gov.au
Cybersmart Program  www.cybersmart.gov.au
Department of Communications  www.communications.gov.au
Raising Children Network  http://raisingchildren.net.au
Safe Schools Hub  www.safeschoolshub.edu.au
Stay Smart Online  www.staysmartonline.gov.au
ThinkUKnow – Internet Safety Program  www.thinkuknow.org.au

ACKNOWLEDGEMENTS
The publisher is grateful to all the contributors to this book for granting permission to reproduce their works.

COPYRIGHT DISCLAIMER
While every care has been taken to trace and acknowledge copyright the publisher tenders its apology for any accidental infringements or where copyright has proved untraceable. The publisher would be pleased to come to a suitable arrangement with the rightful owner.

ILLUSTRATIONS AND PHOTOGRAPHS
Photographs and illustrations courtesy of iStockphoto, except page 2 courtesy of Shutterstock.

THANK YOU
▷ Raising Children Network
▷ Department of Communications
▷ Australian Communications and Media Authority.

DISCLAIMER
The Spinney Press is an independent educational publisher and has no political affiliations or vested interests with any persons or organisations whose information appears in the Issues in Society series. The Spinney Press seeks at all times to present variety and balance in the opinions expressed in its publications. Any views quoted in this book are not necessarily those of the publisher or its staff.

Advice in this publication is of a general nature and is not a substitute for independent professional advice. Information contained in this publication is for educational purposes only and is not intended as specific legal advice or to be used to diagnose, treat, cure or prevent any disease. Further, the accuracy, currency and completeness of the information available in this publication cannot be guaranteed. The Spinney Press, its affiliates and their respective servants and agents do not accept any liability for any injury, loss or damage incurred by use of or reliance on the information made available via or through its publications, whether arising from negligence or otherwise.

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: St Mark's Anglican Community School, Hillarys, libraryadmin@stmarks.wa.edu.au

Issues in Society | Volume 381 Online Safety
INDEX

A
abuse, online 49-50, 51 see also trolling
apps 8, 9, 10, 22, 23, 30

B
banking 19, 20, 22, 23, 29
blocking 7, 8, 17, 25, 38, 42, 48
content 12, 14, 15, 16, 30, 31
blogs 3, 13, 48
Bluetooth 18, 22, 23, 24
Broadcasting Services Act 1992 14, 15, 31
bullying
face-to-face 39, 40
online see cyberbullying

C
chat 5, 7, 9, 11, 12, 13, 31, 33, 43
children’s e-safety commissioner 35, 45-46, 47
Chloe’s Law 46, 47
competitions 19, 21
complaints, making 4, 14, 15, 16, 21, 31, 32, 45, 47
content
illegal 9, 14-16, 19, 31, 32
inappropriate 1, 3, 7, 8, 9, 12, 14-16, 17, 24, 25, 31, 44
offensive 9, 12, 14-16, 17, 19, 25, 31, 32, 36, 37, 42, 43, 48, 49, 51
prohibited 3, 9, 14-16, 31, 32
regulation 1, 4, 31
reporting 3, 16, 43
‘cookies’ 19
counselling 10, 16, 26, 30, 37, 38
cyberbullying 1, 2, 3, 4-5, 7, 8, 10, 13, 24, 33, 34, 36-37, 38, 39-40, 41-43, 44, 45-46, 47, 48, 49
dealing with 33-52
definition 38, 41
parents, strategies for 39-40
victims of 36, 42, 43, 44, 50
young people 41-43, 46
protecting 44, 45
cybercitizens 40, 42
cybersafety 1, 2, 4, 5, 7, 10, 16, 21, 47
cyberstalking 1, 48, 49-50, 51-52

E
email 7, 9, 13, 14, 17, 18, 19, 20, 21, 22,
23, 33, 34, 38, 40, 41, 49, 50
attachments 24

F
Facebook 2, 5, 7, 8, 11, 13, 17, 18, 34, 38, 40, 41, 42, 44, 45, 46, 47, 49, 50
filters 3, 4, 9, 10, 12, 13, 14, 15, 21, 30, 31
‘flaming’ 39, 48
forums 11, 13, 32, 38, 48
fraud 1, 4, 9, 13, 14, 19-20, 23
friends
list 41, 42
requests 16, 17, 41

G
gambling 29-30
games 5, 7, 8, 9, 10, 13, 14, 15, 19, 22,
24, 27-28, 29, 33
gaming addiction 27-28
geotagging 18
Google 45, 46, 47
GPS 24
grooming 7-8, 16 see also paedophilia

I
identity theft 1, 13, 19-20, 22
Instagram 7, 8, 17
internet service providers (ISPs)
family-friendly 3, 11, 15
internet use 3, 33-35, 41, 43
agreements 3, 10, 11
concerns about 12, 13
positive aspects of 3, 11, 12
time limits 3, 10, 11, 15, 28
laws 1, 4, 13, 25, 35, 37, 44, 45, 46, 47, 50, 51
legislation see laws
location settings 8, 18, 23, 33, 50

M
malware 20, 22, 23, 24
MMS 19, 20, 24
mobile applications see apps
mobile devices 1, 3, 7, 10, 18, 22-24,
31, 34
mobile phones 1, 3, 5, 8-10, 18, 19, 20,
22-24, 31, 32, 34, 37, 38, 39, 41, 43
safety 8-9, 22-24

O
online reputation 8, 17-18, 44
online safety
campaigns 1-5
for children 33-35
government policy 35
guide to 7-10
resources 1-5, 10

P
paedophilia 13 see also grooming
passwords 3, 9, 18, 19, 20, 21, 22-24,
38, 41
personal information 1, 2, 12, 13, 16,
18, 19-21, 22, 23, 41, 42, 50
access to 1, 2, 13, 19-21
protecting 17, 19-21
‘phishing’ 20, 23
pornography see also content

R
registrations 19, 21
regulatory measures 1, 35, 44

S
safe zones 15, 16
safety tips, internet 1-32
scams 4, 19, 20, 21, 23, 24
schools, internet policies 3, 7, 10, 11, 36
‘sexting’ 8, 24, 25, 26
shopping 19, 33
shoulder-surfing 22, 23
smartphones 3, 9, 14, 18, 22, 23, 34, 44
SMS 19, 20, 24 see also text messages
social identity, online 7, 44
social media
accounts 17, 18, 50
regulation 35, 44, 45, 46, 47
sites 7, 17, 18, 34, 35, 37, 39, 45-46,
47, 48, 49, 51
use 1, 17, 33-35, 36, 44, 46, 50, 51
social networking 5, 6, 7-8, 11, 13, 42
profiles 23, 41
fake 17, 38, 41
sites 2, 3, 5, 7-8, 10, 11, 13, 15, 21,
37, 38, 41, 42, 47
‘spam’ 9, 19, 20-21
spyware 20
subscriptions 19, 21
suicide 34-35, 44

T
text messages 7, 8, 9, 12, 19, 20, 23, 24,
34, 36, 38, 39, 40, 41, 42, 43, 44
see also SMS
‘trolling’ 7, 48, 49, 51-52
definition 48, 51
‘trolls’ 7, 48, 49-50, 51-52
Twitter 2, 7, 17, 18, 38, 44, 45, 49, 51

V
viruses 13, 22, 23

W
webcams 5, 8, 16
Wi-Fi 22, 23

Y
YouTube 2, 5, 7, 46

This e-book is subject to the terms and conditions of a non-exclusive and non-transferable SITE LICENCE AGREEMENT between THE SPINNEY PRESS and: St Mark’s Anglican Community School, Hillarys, libraryadmin@stmarks.wa.edu.au

60
Online Safety
Issues in Society | Volume 381