父母、监护人和教育者保护在线儿童指南

ITU

www.itu.int/cop

致谢

本指南由国际电联和来自信息通信技术行业主要机构的一组撰稿人起草。没有各位撰稿人奉献的时间和热情，本指南就不可能面世。

国际电联对下述作者牺牲宝贵的时间并提供有价值的见解表示感谢（按姓氏的字母顺序排列）：

- Cristina Bueti和Sandra Pandi（国际电联）
- John Carr（互联网安全儿童慈善联盟）
- Ethel Quayle（英国爱丁堡大学）
- Janice Richardson（Insafe网络）
- Isabella Santa（欧洲网络和信息安全机构）
- Margareta Traung（欧洲安全互联网项目委员会）
- Nevine Tewfik（苏珊穆巴拉克国际妇女和平运动网络和平举措）

作者对来自CHIS的John Carr、UNIDIR的Sonia Billard和Christiane Agbton-Johnson以及ENISA的Katerina Christaki的细心审校和评价表示感谢。

国际电联对eWWG的Salma Abbasi积极参与保护在线儿童（COP）举措表示感谢。

与本指南草案有关的其它信息和资料，请查阅以下网站：http://www.itu.int/cop/，这次资料和信息将定期更新。

如果您有什么意见或希望提供任何附加信息，请通过cop@itu.int联络Carla Licciardello女士 。

目 录

案例研究 — 丧失隐私的风险

互联网使用中的在线风险和薄弱环节

- 社交网络
- 发性短信
- 儿童对新媒体的使用
- 如何获得帮助?
- 教育者如何会面临风险

每个人的责任相同吗?
因人而异传递信息,
家长和监护人可以发挥的作用、
教育者可以发挥的作用、
教育和心理影响、
在线教唆和诱惑、
获取不良在线资料、
可能的问题、
欺辱


保护在线儿童
是一个全球性
问题，因此需要
全球做出响应

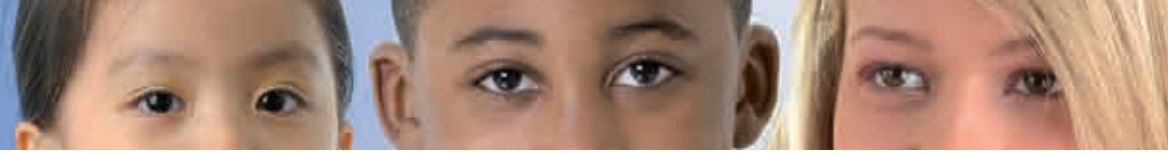
序

很高兴有机会与您分享这份初步指南。本指南是在各利益攸关方的帮助下制定的。

在宽带互联网广泛使用的时代，“保护在线儿童”成为一个关键问题，急需采取全球性措施，协调应对。本地举措甚至国家举措当然有其自身的作用，但互联网没有国界，因此，国际合作是我们赢得所面临的战役的关键。

家长、监护人和教育者对于成功打击网络犯罪和网络威胁至关重要，我谨以个人的名义对大家的支持表示感谢。

国际电信联盟（国际电联，ITU）秘书长
哈玛德•图埃博士



内容提要

互联网给世界各地的儿童带来了前所未有的好处，上网家庭数量逐年增加。到2009年初，网民总数达15亿人，而1998年初，上网人数还不足2亿。

尽管上网的潜在好处不可争辩，互联网亦引发了一些新的和令人烦恼的问题，特别是有关儿童的问题。

今天的年轻人特别通晓技术。他们可以轻而易举地迅速掌握计算机和移动或其它个人装置中的复杂程序和应用，似乎凭本能就可以无所不通；而另一方面，一谈到被多数儿童看作易如反掌的电脑程序和移动或个人装置，成年人普遍需要说明手册。但是，在有关电子安全的辩论中成年人可奉献的是弥足珍贵的生活技能和经验。

查明儿童和青年网上实际作为与成年人的想象有何不同至关重要。研究表明，越来越多的儿童使用游戏机和移动装置上网，而很多成年人尚不知道这些设备亦可用来连通网络。

一个关键的问题是，儿童和青年人往往在成人认为安全的地方上网，如家里和学校。很多家长和监护人都坚持误认为，他们的孩子使用家中计算机上网比在外边上网更安全。这种误解很危险，因为互联网可以将孩子和青年人带到几乎世界各个地方。在此过程中，他们面临的潜在风险与现实世界没有什么不同。

该指南是为保护在线儿童（COP）举措[1]而制定的，构成国际电联全球网络安全议程[2]的组成部分。其宗旨是为今天和未来的青年享有一个安全可靠的网络世界奠定基础。

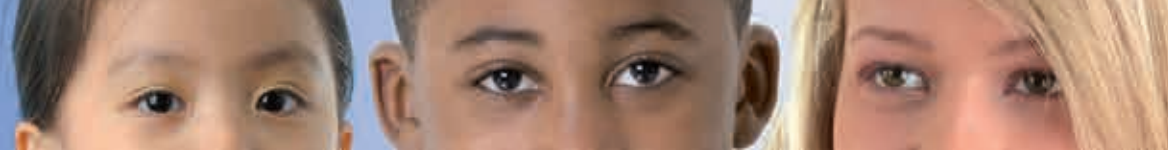
指南旨在提供一个蓝图，

[1] http://www.itu.int/cop

[2] http://www.itu.int/osg/csd/cybersecurity/gca/

《联合国保护儿童权利公约》将18岁以下的所有人定义为儿童。本指导涉及的问题关系到世界各地18岁以下的所有人。尽管如此，一个7岁的互联网用户很可能与刚上中学的12岁儿童或即将迈入成年的17岁儿童具有不同的需求和兴趣。为适应不同情况，指南在多处因地制宜地提出指导和建议。虽然笼统概况的指南具有意义，但不能忘记的是，每个孩子各不相同。每个孩子的具体需求应逐一得到关注。此外，各国或区域不同地方、法律和文化因素也会对指南的使用或解释产生重要影响。

目前保护儿童的国际法律和法规不计其数，多数情况下，规定了保护儿童的一般性行动，同时对有关互联网的行动，还做出了具体规定。这些法律和法规构成本指南的基础。该宣言全面概括了上述法律和法规并呼吁采取行动，防范并终止对儿童和青年的性剥削，2008年11月召开的第三届打击对儿童和青年进行性剥削世界大会[1]通过了《里约热内卢宣言》。



通过调整可适用于各国或地方的习惯和法律。此外，如果指南能够解决可能影响到18岁以下所有的儿童和青年的问题将备受欢迎，但是各年龄段的儿童具有不同的需求。的确，每个孩子都是不同的，需要得到相应的关注。

本指南是由国际电联与一组活跃在ICT行业领先机构的作者编写的。这些机构包括欧盟更加安全的互联网计划、欧洲网络与信息安全局（ENISA）[3]、有关互联网安全的儿童慈善同盟、网络和平举措和爱丁堡大学（英国）。我们还得到很多志同道合的国家政府和高技术企业给予的弥足珍贵的支持。我们的共同目标是使互联网成为儿童和青年人可以享用的更加美好和安全的地方。

国际电联和本报告的其他作者向所有利益攸关方呼吁，促进通过保护上网儿童促进安全获得网络资源的政策和策略。

这不仅有助于建设更具包容性的信息社会，还能使国际电联成员国得以履行联大1989年11月20日第44/25号决议通过的《联合国儿童权利公约》[4]和WSIS成果文件规定的保护和实现儿童权利的义务[5]。

[3] http://www.enisa.europa.eu

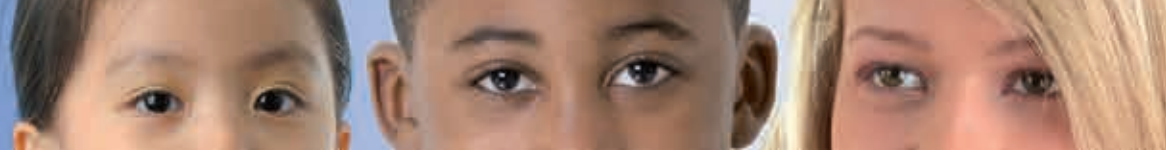
[4] http://www.unicef.org/crc

[5] http://www.itu.int/wsis/outcome/booklet.pdf

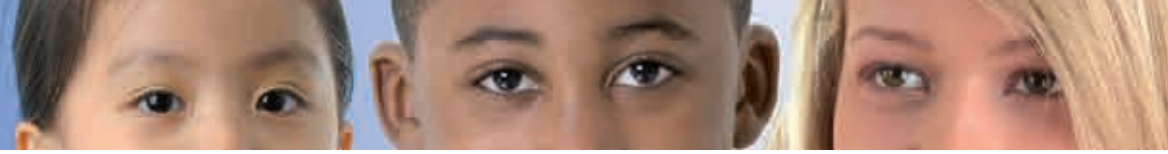
家长、监护人和教育者指南

本节旨在为家长、监护人和教育者提供指南，从而使他们帮助孩子在网络世界中获得安全而有益的体验。第49页更全面地列举了需考虑的问题。

家长、监护人和教育者		
	#	需考虑的主要问题
1. 个人电脑的安全和可靠性	a.	将计算机放在一个公共房间
	b.	安装防火墙和防病毒软件
2. 规则	a.	就互联网和个人装置的使用达成内部规则，特别注意隐私、年龄不当、欺辱和陌生人的问题
	b.	制定有关使用移动设备的规划



3. 教育家长、监护人和教师	a.	家长、监护人和教师应了解孩子使用的网站及其如何度过网上时光
	b.	家长、监护人和教育者应了解孩子是如何使用手机、游戏机、MP3播放机、PDA等其它个人装置的
4. 教育儿童	a.	教育子女有关交流个人信息、安排与网上结识的会面、在网上公布照片、使用网络摄像头等做法的风险
5. 沟通	a.	与子女沟通体验情况



1. 背景

在日内瓦（2003年12月10-12日）和突尼斯（2005年11月16-18日）分两个阶段召开的信息社会世界峰会（WSIS）勇敢地做出承诺：“建设一个以人为本，具有包容性和面向发展的信息社会，在此信息社会中，人人可以创造、获取、使用和分享信息和知识”（《日内瓦原则宣言》第1段）。

在WSIS上，国际电联被国际社会领导人责成执行C5行动方面，“树立使用ICT的信心并提高安全性”。

WSIS在成果中还特别认识到儿童和青年人的需求以及对他们在网络空间予以保护的必要性。

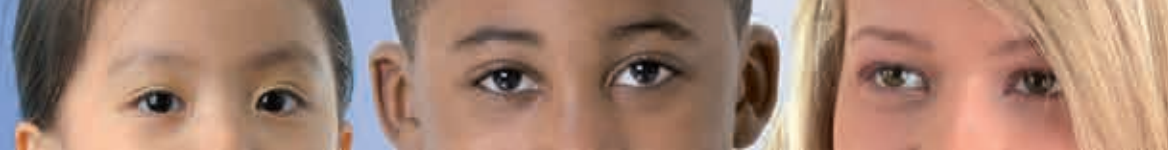
《突尼斯承诺》认识到“信息通信技术在保护和促进儿童成长方面的作用”以及“采取更有力的行动以保护儿童在信息通信技术方面的权利，避免他们因为这类技术而受到虐待的必要性。”

习以为常的是[6]，我们每天都知道孩子的去向，和谁在一起，以及他们在做什么。

但连最小的孩子都日益迷恋的数字世界中，我们常常仅能退而观望，很多人被“数字鞭子”指挥得晕头转向。

[6] http://www.parenting.com/article/Mom/Relationships/How-to-Spy-on-Your-Child-Online


成人将生活技能
和经验带到有关
电子安全的辩论中



儿童，哪怕是年龄很小的孩子，都可能比教育者或家长了解今天的技术。

今天的儿童只体验过数码世界，在这个世界中技术体现在他们生活的方方面面。

数码世界给了他们友谊，教育和对世界的以及周围人的认识。与此同时，作为成年人，我们却在为确定哪些规则和如何执行规则一筹莫展。

问题是，这个议题不在家长手册内，这一章节尚未编写，而社会还未来得及为此制定标准。

我们有法定饮酒年龄和法定驾车年龄，但有关儿童独立安全上网或用手机给朋友发送短信的年龄或就家长在监督脆弱且常常过于单纯的孩子的上网活动中的作用，尚无惯例可循。

家长的想象和孩子的能力具有天壤之别。

尽管92%的家长指出，他们已对孩子的上网活动设定了规则，34%的儿童表示，其家长无所作为。这种情况在世界很多国家比比皆是：

在法国，72%的儿童独自上网浏览，尽管85%的家长知道存在家长控制软件，只有30%的家长安装了这种软件。

在韩国，90%的家庭拥有廉价高速宽带连接，18岁以下的青少年中30%几乎上网成瘾，每天上网时间超过2小时甚至更长。

在英国，9-19岁中的57%表示，他们已见过网上的色情内容，46%的人表示，他们已发送过不该给出的信息，33%的人表示，他们曾在网上受到欺负。

在中国，44%的儿童表示，他们曾在网上遇到过陌生人，41%的人已和网上陌生人谈论过有关性的问题或难以启齿的问题。

为应对这些挑战，国际电联及其它利益攸关各方于2008年11月推出了保护在线儿童（COP）[7]的举措。

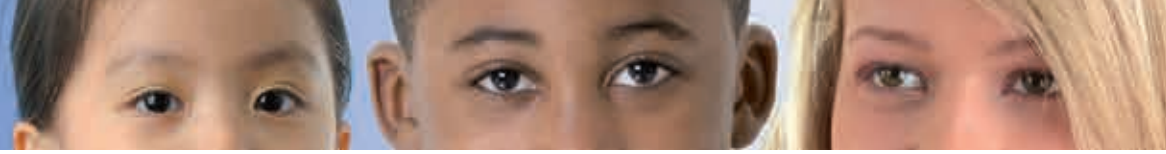
COP是国际电联全球网络安全议程（GCA）[8]的一部分，是全球用来采取促进保护在线儿童和青年行动的合作网络和其它联合国机构和伙伴一起，该举措为安全在线行为提供指南。

[7] www.itu.int/cop
[8] www.itu.int/osg/csd/gca

COP举措的主要目标是：

- 确定网络环境中儿童和青年面临的风险和薄弱之处；
- 通过多种渠道提高对这些风险和问题的认识；
- 开发实用工具，帮助各国政府、各组织和教育者降低风险；
- 分享知识和经验，同时促进国际战略伙伴关系的建立，从而确定并实施切实可行的举措。

- 国际电联围绕保护在线儿童（COP）举措拟定的指南旨在为家长、监护人和教育者就保护在线儿童提供信息、建议和安全常识。



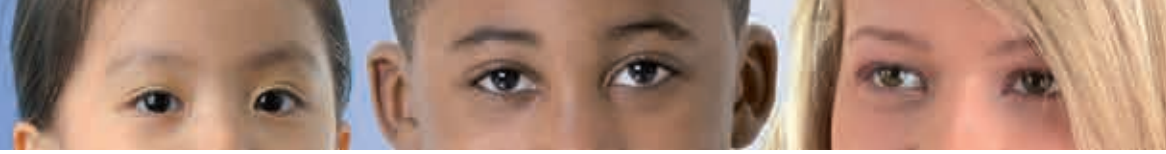
2. 网上的儿童和青年

互联网在近年内一直保持高速发展。博客、维基、My Space、You Tube和在线游戏等新服务提升了互联网的连通性，使社交网得到进一步发展，让浏览者得以创建自己的内容。在过去两年中新博客每五个月翻一番，社交网络网站（如Bebo、Facebook,、Habbo和Twitter）的使用率逐年成倍增长。在过去三年中，网络用户之间的通信已成为互联网流量的最大来源。

儿童和青年是ICT的钟情用户，他们使用ICT聊天和分享个人信息。这为参与、创新和教育带来了多种多样的良性机遇，同时也使青年人得以跨国家、宗教和文化边界开展交流。举例而言，以下表格描述了儿童在进入虚拟世界后所体验到的情况[9]：

[9] ENISA，虚拟世界中的儿童 – 家长应知道的，2008年9月，可查阅以下网站http://www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf

角色类型	兴趣所在	扮演者	特点
探寻 – 侦探	跟踪搜寻，解决疑难问题，出外旅行，从事“户外运动”	更有自信的儿童，没有年龄或性别差异	追求细节、好奇、善于沟通，在破解谜团中发挥想像力
我封名号者	在数字世界中表现自我	男女兼有，年龄较大者可能居多	男孩和女孩都希望在其化身上制造标记，有时使用自己的头像；大一些的女孩愿意在打扮后形成化身。男孩或女孩都希望创建一个家或“基地”来表现自我
攀高枝者	一定环境内的档次和社会地位	不论年龄大小，性别上略有差异（男孩比女孩表现略突出）	有竞争力、关心社会排位并将此排位展现给他人
角斗士	死亡和破坏、暴力、和超级强势	男性、多为年龄较大男孩	在没有办法表达自己时，儿童表现出愤怒，有机会“赢取”并“战胜对方”可减轻愤怒



角色类型	兴趣所在	扮演者	特点
收藏消费者	收集某个体系内所有具有价值的东西	年龄较大的男孩和女孩	收集纸页和硬币、寻找商店、获奖机会、积蓄和存放个人物品的地方
超凡用户	将知识和经验的好处给予每个人	熟谙游戏、环境地理和相关系统	每次花若干小时玩游戏，最感兴趣的是探寻游戏的工作原理
生命系统建设者	在环境中开辟新天地、新内容，在环境中安置人口	年龄较小的儿童（毫无约束地想像世界）和年龄较大的儿童（按条条框框系统地想像世界 – 房屋、学校、商店、交通、经济）	在没有办法表达自己时，儿童表现出愤怒。拥有（或没有）这种掌控环境的方法具有吸引力
养育者	看护自己的化身和宠物	年龄较小的男孩和女孩及年龄较大的女孩	儿童希望与他人会面并玩耍，向其化身教授游戏等技能并为其化身安排睡眠的地方。虚拟宠物亦受青睐

互联网是一个中立的手段，在分发数据上良莠不分。

一方面，对教育不同年龄和能力的人，它蕴藏着巨大的潜力。

而在另一方面，互联网可用来设置网上陷阱，利用用户从事犯罪行为。不幸的是，儿童就是最容易落入这种陷阱的脆弱群体。

必须牢记的是，互联网不是唯一可以对儿童的成长造成不良影响的通信手段。

在过去几年中，年轻人对移动电话的使用迅速增加，而且，儿童正在使用移动电话随处上网。这将加大其在无成人监护的情况下面临网上危险的可能。

举例而言，在韩国，儿童获得第一部手机的平均年龄为8岁。

不得忽视的是，移动电话本身近年也有了很大发展。

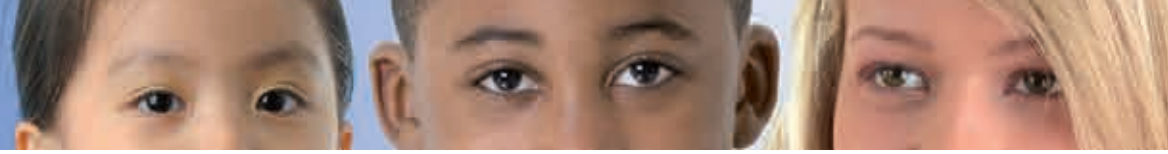
手机现在可以用来传递视频信息、提供娱乐服务（下载游戏、音乐和视频）以及上网并获取基于位置的服务。

儿童通过手机或其它个人装置上网的潜在风险与通过有线连接上网的风险几乎相同。

通过儿童手机或手提电脑与传统上通过家用电脑上网的最大差别是这种个人移动装置具有很强的私密性。

十几岁的孩子在使用个人装置时，家长一般无法像在家中使用电脑一样给予监督。

家长应就手机的使用与孩子交流，确保他们能够在购买了手机或在手机首次得到使用时就加以控制。



案例研究：埃及的青年和互联网

埃及青年互联网安全焦点组（Net-Aman）由11位18至28岁的成员组成，是更为广泛的网络和平举措不可分割的一部分。该举措是在一系列合作伙伴支持下，由苏珊穆巴拉克妇女国际和平运动创建的。

焦点组的名称为Net-Aman（阿拉伯文意为“网络安全”），该名称是由青年成员挑选的。

该组的职责范围是提高人们对互联网安全和巨大ICT潜力的认识，目的在于向儿童和青年提供自我识别有害内容并通过参与决定最佳处理方法的机会。

Net-Aman的首场培训产生了一份问卷调查表，由此，成员就可对儿童和青年有关在埃及使用互联网的担忧及希望“一目了然”。

每位青年都有责任走入学校和大学，就调查结果向2008年3月举办的第二场培训提供一份报告。该调查涉及一系列年轻人，代表了从8至22岁不同年龄组的人群。

这种调查有助于Net-Aman了解了埃及青年对互联网及其安全性的感受。

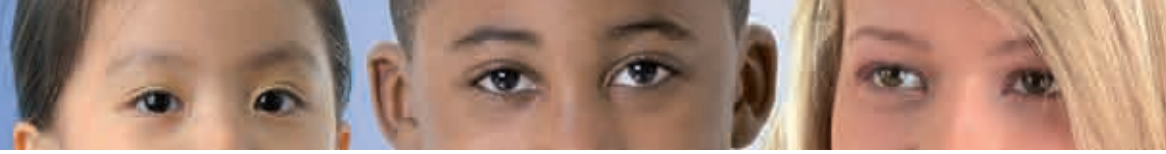
约800名埃及青年对题为“埃及青年与互联网”的青年对青年的调查做出了回应。

被调查的儿童和青年指出：

- 他们在使用互联网时，没有成年人的监控。
- 有关在埃及使用互联网的风险和挑战，他们列举了以下内容：不当内容代表主要的在线风险，之后是病毒和间谍软件、暴力内容、家庭作业复制（抄袭）最后一项风险是网络欺辱。
- 调查中最令人震惊的结果之一是，大多数青年分享其个人信息，包括全名、年龄、照片、学校信息和电话号码，而对后果毫不担心。

根据此次调查的结果并按照埃及青年互联网安全焦点组Net-Mman的职责范围，青年成员将继续努力，帮助人们为了埃及青年提高对保护在线儿童问题的认识。

预了解更多信息，请访问以下网站：http://www.smwipm.cyberpeace initiative.org



3. 家长、监护人和教育者

家长、监护人和教育者的定义

一些互联网网站笼统地称谓家长（如“家长网页”和“家长控制”），因此，有必要将在理论上能确保儿童安全并负责任地使用互联网网站并能对儿童访问具体互联网网站给予许可的人定义为家长。

在此文件中，“家长”一词指自然母亲和/或父亲或获得监护权的人。

今天的世界包罗万象，很多孩子的抚养人并非自然父母。

他们经常被称为监护人或抚养人。必须认识到，对于在其监护下而言，上网的孩子他们可能发挥的作用。

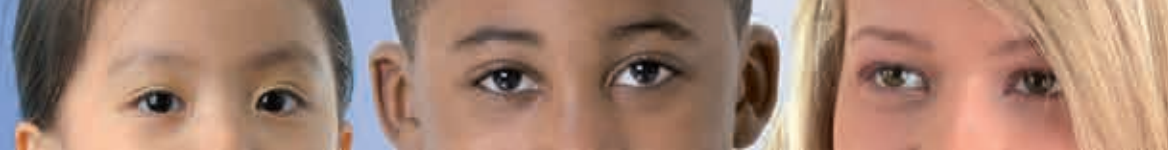
教育者是通过系统工作提高他人对问题理解的人。

教育者的作用体现在课堂的教学和非正式教育两个方面。举例而言，他们可以在社交网站上提供在线安全信息或在社区或学校组织课程，使孩子安全地畅游在网络世界中。

教育者的工作根据其工作环境和儿童（或成人）年龄组的不同千差万别。

他们包括所有与孩子和青年接触的人 – 家长、教师、社会福利提供者、图书馆服务、家务工人、青年领袖以及包括祖父母在内的广义家庭成员。值得一提的是，享受社会服务的孩子是特别脆弱的人群，因此需要特别关注。

此外，还要重视同龄人的影响 – 因为这些人在某种意义上充当了教育者。



很多家长、监护人和教育者尚不知道

ENISA最近进行的分析显示，在多数情况下，家长和监护人不了解他们的孩子可能遭遇的在线经历以及在各种在线活动中面临的风险和薄弱环节。

儿童可以使用不同的平台和装置上网，其中包括：

1. 个人电脑
2. 移动电话
3. 个人数字助手(PDA)。

根据所用的平台类型以及现有的功能，每个人的体验都将与众不同，举例而言：

功能	描述
建立资料	输入本人信息
与他人的互动	与其它用户通过聊天、博客、即时消息、讨论论坛和互联网协议话音（VoIP）功能交流信息和想法
创建化身	选择代表自己的图形形象，在互联网站上建立身份。
玩游戏	挑战智力，提供在线参与活动。
回答测试	头脑风暴等挑战通常给参与者以奖励。同时，在朋友或朋友圈之间用“计分板”的形式开展竞争。
制作图画、动画、漫画和小工具	也被称为UGC或用户生成的内容，很多儿童喜欢创建自己的内容，然后与伙伴分享。在虚拟社会中，在与他人合作时努力发挥创造力。
创建内容，从音乐和舞蹈到视频	自助出版适用于各年龄段的孩子，是展示创造力的良机。
购买产品	一些服务可让用户使用真正的货币购买产品或服务。
上传照片或其它信息	有些服务可允许儿童上传照片和信息，其中一些会过滤个人信息和/或其它不良内容。
下载音乐	一些服务可允许儿童下载音乐
观看有关产品/服务的广告	互联网站通常是靠做广告维持运行的。

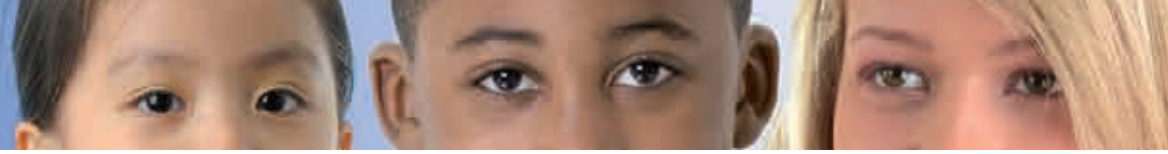
年轻人上网的原因五花八门，其中包括（10）：

1. 在新的环境中结识朋友，与他人就共同的兴趣实时交流。
2. 创建并加入社团或兴趣小组，如音乐、足球等。通过博客、即时消息和其它手段围绕相关兴趣领域沟通思想和信息。
3. 结识新人并最终结交新的朋友。
4. 创建并共享原创个人内容，如图像、照片和视频，扩大自我表达机遇。
5. 创建、发表和分享音乐。
6. 玩游戏
7. 建立自己的空间，甚至在家长和抚养人在场的情况下。
8. 尝试身份、新的社会空间和各种极限。

虽然通过移动电话或PDA上网与通过个人电脑上网的体验有所不同，但无论平台如何，使用互联网的风险和薄弱环节基本相同。

一个关键的问题是，儿童和青年往往是在我们所说的安全地方上网的，如家里或学校。家长和监护人也有同样的误解。他们总是说，更愿意孩子们在家中使用电脑，而不是在外边。否则，他们将不知道孩子身在何处。当然，互联网可以将儿童和青年带到任何地方，他们可以像在现实世界一样面临各种风险。（见21页的案例）

[10] 家庭办公：有关保护在线儿童的家庭办公任务组-2008年社交网络和其它用户互动服务提供者最佳做法指南，见以下网站 http://police.homeof¬fice.gov.uk/publications/operational-policing/social-networking-guidance?view=Binary（最后访问日期为2008年6月16日）



案例研究：丧失隐私的风险

很多用户从未意识到他们在网上给出了个人信息，或甚至不知是如何给出了这些信息！

- 这些方法包括：
- 忘记点击隐私设置，
- 给出的信息多于要求的信息

然而，对于儿童和青年人，这可以使他们面临同伴、更大的青年或甚至成人的不当接触。儿童还可能无意识地给出了有关自己的信息：

- 通过填写任何表格（如比赛和注册）
- 公布个人资料
- 创建网站

重要的是，家长不得以我们讨论孩子可能在网上面临的风险的方式夸大这些风险，或对孩子进行不适当的恐吓。

儿童会如何无意地在网上给出信息，以及这些有关他们的信息如何被陌生人发现是我们要考虑的重要问题。

儿童需要了解的是，能够提供有关其地址、电话号码和电子邮件地址的数据库比比皆是。

应鼓励儿童和青年在上网时始终使用隐私设置，并在被问及个人（具体）信息时或在网上沟通期间遇到困难时，向负责任的家长发出告警信息。

以下是一个模拟聊天室的讨论，执法人员认为他可以代表现实生活中的在线讨论。假设一个伺机做案的恋童癖进入聊天室注意到这个孩子，之后使用该信息对其诱惑，您的孩子是否会上当？不幸的是，一些孩子就会陷入圈套。

孩子：我恨我妈妈！我知道父母离婚都是因为她。

猎食者：我知道，我的父母也离婚了。

孩子：我们再没有钱了。每次我需要东西时，她总是说：“我们买不起”。当父母在一起时，我可以买东西。现在不行了。

猎食者：我也一样，我很痛恨！

孩子：我等了六个月才等到新的电脑游戏。我妈妈曾经承诺在游戏出来时为我买一套。她承诺过！现在游戏出来了，我还能买吗？不可能。“我们没有那么多钱”。我恨我妈妈！

猎食者：哦！太糟糕了！我拿到了！我有一个叔叔很

酷，他总是给我买东西！他很有钱。

孩子：你太幸运了。多希望我也有一个这么好还有钱的叔叔。

猎食者：嘿，我有主意了！我问问我叔叔能不能给你也买一套...我跟你说过他真的很好。我敢保证他一定同意。

孩子：真的吗！？太谢谢了！

猎食者：很快BRB[网络语言“很快回来”]...我去给他打电话。

猎食者：你猜怎么着？他同意了。他已经去给你买游戏了！

孩子：哇，真的吗？谢谢，我真的不敢相信！

猎食者：你在哪儿住？

孩子：我住在新泽西，你呢？

猎食者：我住在纽约。我叔叔也在纽约。新泽西不远。

孩子：太棒了！

猎食者：你家附件有商业中心吗？我们可以在那儿见面。

孩子：好，我住在GSP商业中心附近。

猎食者：我听说过。没问题，星期六怎么样？

孩子：太好了。

猎食者：如果你愿意，我们也可以去麦当劳。我们可以中午在那儿见面。

孩子：好的，在哪儿？

猎食者：在电脑游戏店前。对了！我叔叔叫乔治。他真的很酷。

孩子：太好了...谢谢。我真的很感谢。你太幸运了，能有这么有钱的好叔叔。

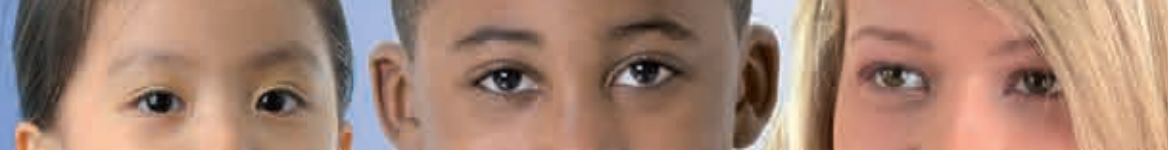
星期六，孩子来到商业中心，在电脑游戏店外面遇到了一位成年人。他自称为“乔治叔叔”，而且解释说，他的侄子已在麦当劳等待他们。

孩子感觉不妙，但这位叔叔走进商场，买了价值*100*美元的游戏。他走出来把游戏交给孩子，孩子立刻放松下来，而且万分愉快。

提醒当心陌生人的警告是没有意义的。因为他不是陌生人，他是“乔治叔叔”，而且，需要证据的话，电脑游戏就是证据。孩子毫不犹豫地进了乔治叔叔的汽车，去麦当劳见他的朋友。接下来的事情成为*6*点新闻的报道内容。

这个故事令人作呕。它使我们浑身感觉不适，但它的确发生了。虽然这种事情并非接连不断，但是屡次三番足以使人敲响警钟。（每年抓获和关押的网络猎食者达几百人）。如果轮上您的孩子，一次就将造成灾难。了解猎食者的做法和伎俩有助于教育孩子如何避免上当受骗。

来源：http://www.wiredkids.org/parents/parry_guide.html



互联网使用中的在线风险和薄弱环节

面对非法和有害内容，如色情、赌博和其它对儿童不利的内容以及与其他网民的接触。在多数情况下，这些网站的运行者未采取有效措施，限制儿童进入其网站。

非法和有害内容的创建、接受和传播。

冒充他人，往往是另一个孩子，作为有意伤害、束缚和欺负他人的手段。

不当接触，特别是与冒充孩子的成人的接触。

个人信息披露导致的人身伤害风险。

假冒互联网用户为牟取金钱试图犯罪。在一些情况下，这可能包括身份窃取，尽管这种做法通常涉及欺诈成人的行为。

通过与在线伙伴实际接触造成人身伤害，身体或性伤害均有可能。

通过垃圾信息和公司广告使用互联网网站寻找目标，推广抗衰老和/或相关产品。

过量使用对社会和/或室外活动、信心提高、社会发展和大众健康造成不利。

欺负和骚扰。

自残、破坏和暴利行为，如“快乐打耳光”。

强迫或多过使用互联网或在线游戏

面对种族主义和其它歧视性言论和形象。

诋毁和损坏声誉。

通过剽窃和未经允许上传内容（特别是照片）侵犯自身或他人权利。未经许可取得并上传不当照片证明对他人造成伤害。

通过下载音乐、电影或应付费的电视节目对他人版权造成侵害。

依赖或使用网上找到的不正确或不完整信息，或来自未知或不可靠来源的信息。

未经授权使用信用卡：家长或他人可用来支付会员费、其它服务费和商品的信用卡。

错误显示个人年龄：或孩子冒充年龄较大者以便进入与个人年龄不符的网站，或年龄较大者为了同一原因从事冒充行为。

未经同意使用家长的电子邮件账户：在需要家长认可启动虚拟世界儿童网站时，孩子可能滥用家长账户。一些服务账户一旦启用，家长很难删除。

不良广告：一些公司通过虚拟世界网站向儿童发送垃圾信息以销售产品。这引发了用户认同的问题以及如何获得认同。由于该领域法律不健全，所以很难确定儿童何时才能理解数据交易。的确，如何在互联网中应用这些规则已经令人头痛，而使用手机上网使问题变得更加复杂。

具体到教育者，以下情况令其担忧，因此他们常常感到束手无策：

社交网络 – 儿童和青年使用社交空间生活的方式与众多教育者所熟悉的方式大相径庭。很多人无法理解为什么在一个联络名单中会有如此多的“朋友”，朋友量被年轻网民看作人缘状况。

发性短信 – 这是一个较新的现象，儿童和青年通过在网上公布个人性感形象或使用移动技术向朋友发送，使个人陷入危险之中。

儿童对新媒体的使用与我们的想象完全不同。目前开展的一些研究工作（不同国家）可对我们提供帮助。（另外，请在以下网站查阅欧盟问题摘要中有关欧盟在线儿童的情况：www.eukidsonline.net）

如何获得帮助？很多国家设立了帮助热线，由此儿童和青年可以报告问题。这种做法很普遍，不同国家采用不同的方法传递信息。重要的是，儿童和青年人必须认识到，什么时候报告问题都不迟，通过报告，他们就可对他人提供帮助。

教育者如何会面临被欺负风险（如儿童和青年创建了有关仇恨教师或其他专业人员的网站）。教育者需要树立信息，他们可以安全地使用技术。很多教育者认为没有能力应对这些问题，因此不知如何将材料辙出网站。今天的教师网站在此领域和其它相关议题上提供了出色的指导：

www.teachtoday.eu

必须强调（如上所述）的是，尽管一些教育者对技术不如儿童和青年熟练，但他们具有充足的生活技能和经验，因此可以提供建议、指导及支持。在向教育者提供有关电子安全问题的培训时，有必要反复强调这一点。

然而，OPTEM研究[11] 显示，儿童自己发现的风险多与互联网相关，而非移动电话，其中包括：

计算机风险（如病毒和黑客）

推介性图像的出现、或误入充满暴力或色情的不良网站。（年龄大一些的儿童总是淡化意外遭遇的影响）。

不利因素和欺诈

居心叵测之人发动的性攻击。

虽然儿童认识到他们有时会允许自己陷入危险行为，但对这类行为产生的风险并不担心，同时表

[11] http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/qualitative_study_2008/summary_report_en.pdf

现出要自行或在其同龄组内解决问题的意愿。只有在遇到可能出现的“大事”时，他们才会找到家长或成人。大一些的男孩尤其如此，他们可能会使用担忧按钮[12]（如虚拟全球任务组开发的按钮）。然而，并非所有孩子都是这种情况。我们可以看到，认识到风险的孩子知道“保护”自己的活动，但是通常不与他人交流新技术的看法。这些技术往往要求家长对青年人的行动做出评判和监督[13]。我们需要在简单地区分脱机和在线世界时谨慎从事。因为这样无法体现出我们的生活与在线技术如何息息相关。对于很多儿童而言，这意味着有必要仔细权衡技术给予的机遇（如探索身份、建立密切关系和提高社交能力）和风险（有关隐私、误解和滥用做法）[14]。

每个人的角色相同吗？

必须牢记的是，对于儿童和青年，教师和家长是学习的主要支持力量[15]。

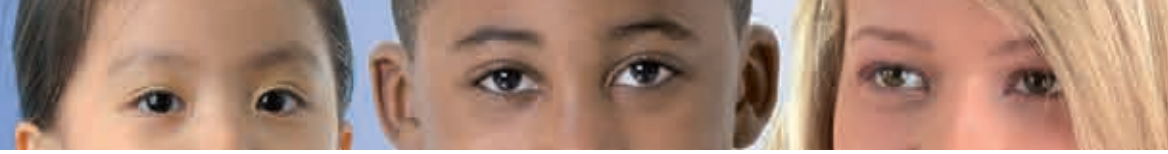
英国拜伦报告[16]表明，儿童保护政策应包括提高认识宣传，支持不熟悉技术的成年人（家长、教师、监护人）学习知识，同时提高儿童的能力，鼓励他们思考安全问题并减少冒险行为。

因地制宜的传播信息

这种宣传的主要目的是改变行为，包括鼓励儿童采用更安全的方式上网，鼓励家长在网上发挥行之有效的作用并鼓励与儿童交往的其他人（大家庭成员、教师等）教授儿童安全上网的方式。

儿童的互联网安全问题不是一个孤立的问题，它与有关儿童、儿童安全和互联网的系列举措拥有很多共同之处。

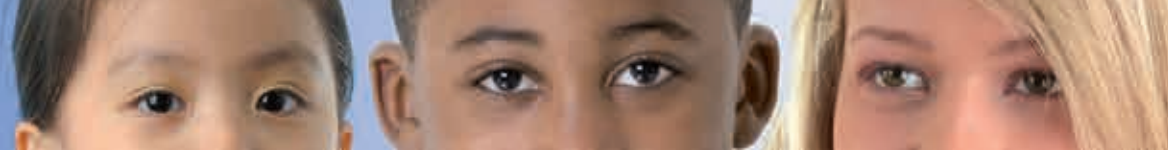
[12] http://www.virtualglobaltaskforce.com/
[13] Quayle, E., Lööf, L. & Palmer, T.（2008年），儿童色情和儿童在线的性剥削，曼谷ECPAT国际机构。
[14] Livingstone, S. 在青年内容创作中承担风险：十几岁的孩子使用社交网站建立亲密关系、隐私并完成自我表达。新媒体和社会，10 (3)，2008年，393-411页。
[15] Livingstone, S., Bober, M. 英国儿童走向在线世界，有关主要项目结果的最终报告，2005年4月。
[16] Byron, T.（2008年）数字世界中更加安全的儿童。



家长和监护人可以发挥的作用

为确保儿童安全并负责任地使用互联网，家长和监护人可以：

1. 与其子女对话，了解他们在使用计算机或者像移动电话或游戏机一类的个人装置时，做什么以及和什么人交流。从保护儿童的角度看，进行并持续这种对话至关重要。
2. 在其子女进入网站前，和他们一起阅读使用条件和须知，一同讨论需要注意的安全预防措施，规定一些基本规则并监督使用，以确保规则能够得到遵守。
3. 教育年轻用户通常应如何负责任地使用技术，鼓励他们听从本能支配并利用自己的判断力。
4. 检查并了解相关网站是否使用下列技术解决方案，如：
   - 过滤器和家长控制。
   - 保留用户记录。
   - 管束（moderation）情况，如果有管束的话，是通过人工还是自动方式进行的，例如，是否使用将识别具体字形和URLs的文本过滤？相关网站是否混合使用人工介入和技术手段？为确保安全和适当的环境，人工管束人员都经过培训。在虚拟世界中，主动管束方通常以角色或参与者的身份出现，或者，在游戏的环境中，可能以游戏主持人的形式出现，无论哪种情况，对于所有用户而言，他们都是看得到的。通常，游戏主持人只是在出现困境时才进行干预，但在一些游戏中，他们对那些看起来“输了”或者需要帮助的用户提供帮助。沉默的管束人员通常身处幕后，阻断攻击性资料，对可疑行为做出反应，警告用户，并开展其它管理监督活动。
   - 如果相关网址允许公布照片或视频资料，该网站是否积极管束这些内容，或者它是否仅在收到报告之后才审查图像？
   - 报告和阻断功能：通常是报告公布不适当内容、进行不适当会话与活动的工具，如“设置标记”和“报告按钮”等。虚拟世界亦应显示如何报告不适当行为以及向谁报告的明确政策。应教会儿童如何报告相关事件或不需要的接触以及如何阻断不需要的接触，如何使用隐私设置以及如何记录在线会话。
   - 分级：家长和监护人应了解分级符号及其使用，将此作为保护年轻用户不受不适当服务和内容影响的一种重要工具。
   - 年龄确认：如果一个网站声称使用年龄确认，那么它的系统是否健全？如果出售有年龄限制的产品的话，是否采用了一种可以确定人的年龄的可靠年龄确认系统？



5. 坚持参加在线年轻用户的活动。强调家长和儿童照顾者在互联网站中可以并应该发挥作用的重要性十分必要，因为他们的参与对于其子女的经历极具影响力，有利于形成积极的行为举止。
6. 如果听到或看到任何引起您关切的有关您孩子的行为或其在线朋友行为的事情，请保持镇定，不要乱下结论。对于一些年轻人而言，一些互联网网站相当于社交生命线。如果您孩子担心您将直接切断他们的社交生命线，他们可能更不愿提及他们可能面临的问题或关切的事情。
7. 应当清楚的是，您孩子的在线行为可能同与您面对面时的非在线行为大有所异。人们在线时表现得更为咄咄逼人，这并非少见，因为他们认为没有人会要求他们承担责任。应利用任何有关您孩子不适当行为的情况报告来与您的孩子讨论在线交流的适当口吻。
8. 了解在线文化，这样，在出现需要年轻人为自己的在线行为负责的情况时，您就可以判断出年轻人所给的典型借口是否真实可信，如，“有人偷了我的账户”等。但是在违反虚拟世界规则的消息和聊天记录方面则很少出现此类情况。可能会出现，但是相当例外。
9. 教育您的孩子不要与朋友或兄弟姐妹共享其接入密码。这是年轻人在互联网网站方面所面对的最大问题之一。例如，兄弟姐妹的一个最好的朋友可能会窃取您的孩子费尽千辛万苦收集到的虚拟资料。
10. 利用网站的联络页面来共享您的关注和问题。网站有责任确保您能对网站放心使用。
11. 不要想当然地认为互联网上的每个人都以您的孩子为目标。统计数字表明，非在线时出现的恋童癖患者问题远远超出了在线时的问题。一般而言，儿童网站比较安全，而且可以为您的孩子提供美好的、富有创造性的社会和教育经历，但是你仍须参与而且了解情况。

教育者可以发挥的作用

重要的是，教育者不应对儿童和年轻人可能了解或不了解哪些网络安全方面的问题做出假设。对于互联网以及哪些是适当还是不适当的做法，人们存在误解。例如，许多十来岁的年轻人相互之间共享密码，而且这通常被认为是一种真正友谊的标志。

教育者的一项重要作用是，教育儿童和年轻人密码的重要性，如何保证密码安全以及如何创建一个更强的密码。

同样，在版权问题方面，年轻一些的用户对于下载非法音乐和视频显然关切不够，许多成年人对此感到震惊。研究[17]表明，儿童和年轻人不仅不关注版权问题，而且对与在线版权内容合法性相关的问题更缺乏了解。这也是教育者可以发挥明确作用、并向学生做出解释的另一个方面。

[17] 哈佛大学伯克曼互联网与社会研究中心。-- John Palfrey 和Urs Gasser--2008年

学校有机会进行教育改革，帮助学生发挥其潜力并提高ICT方面的水平。然而，同样重要的是，儿童需要了解如何在使用这些新技术（尤其是像社交网站类的WEB 2.0协作技术）时，保证安全。此类技术正在成为有成效的创造性社会学习的一项基本内容。通过以下方法，教育者可以帮助儿童明智、安全地使用技术[18]：

1. 确保学校有一套健全的政策和做法，并定期对这些政策和做法的有效性进行审议和评估。
2. 确保人人都了解可接受使用政策（AUP）及其用途。重要的是制定针对适当年龄的可接受使用政策。
3. 检查学校的打击欺辱政策是否提及利用互联网和移动电话或其它装置进行的欺辱，而且在出现违背该政策的情况时，是否可进行有效制裁。
4. 指定一名电子安全协调员。
5. 确保学校网络安全可靠。
6. 确保使用获得资格认证的互联网业务提供商。
7. 使用过滤/监控产品?
8. 对所有儿童进行电子安全教育，并明确说明进行此教育的地点、方式和时间。
9. 确保所有教职员工（包括教学辅助人员）均接受适当的培训，并定期进行更新。
10. 在学校确定一名联系人。收集并登记电子安全方面的事件可以使学校更好地了解需解决的问题或出现的任何趋势。
11. 确保管理团队和学校校长对电子安全问题有足够的了解。
12. 对所有电子安全措施进行定期审查。

教育影响和心理影响

近年来，儿童使用互联网技术的势头发展迅猛，这带来了人们对在线安全问题的日益关注。从历史上看，对于交流技术所带来潜在危险的精神恐慌不断出现，对于年轻妇女而言，情况尤其如此。但是，有人认为，在对这种危险真正展开调查时，看来往往并不是技术本身带来的问题，而是相关儿童机构利用技术及失去家长控制所带来的焦虑引起的关注[19]。人们一直认为，教育者在推进和确保互联网安全方面发挥关键作用。世界上的家长似乎均认为学校应该在教育儿童使用安全技术方面发挥中心作用，而且儿童慈善会也建议，“应该向学校提供有关安全使用互联网、电子邮件、聊天室、学校网站以及过滤和阻挡软件的更为明确的指南”[20]。

[18] BECTA。保护在线儿童。2009年。

[19] Cassell, J. & Cramer. M. 高技术或高风险：有关在线女童的精神恐慌。在T. McPherson (Ed.)中，数码青年，创新，以及未预料到的情况。有关数码媒介和学习的John D. 和Catherine T. MacArthur基金会系列。剑桥，麻省：麻省理工学院出版社，2008年，53-76页。

[20] 互联网安全联盟儿童慈善会（2001年）。为了儿童，努力使互联网成为安全之地。见：www.communicationswhitepaper.gov.uk/pdf/responses/ccc_internet_safety.PDF

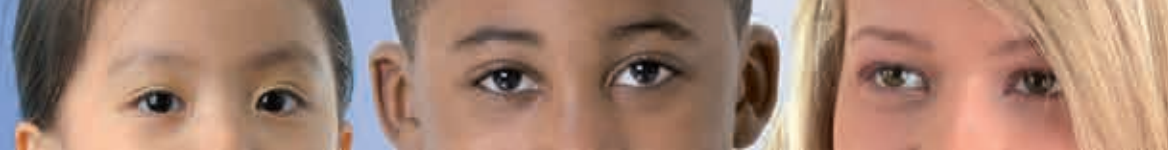
早期开展的有关在线安全的工作主要集中在使用过滤软件等技术解决方案上，但是，近期以来，信息技术日益移动化，其结果是，桌面电脑已不再是上网的唯一接入点。目前，数量日益增长的移动电话和游戏机均有宽带连接，而且儿童可以在学校、家中、图书馆里、互联网吧、快餐店、青年俱乐部，甚至在上学的公共交通工具上均可以上网。学校提供的利用互联网的机会，通常是在封闭网络或在周围有其他儿童的情况下进行。明显措施包括：确定网络能够有效安全，但我们需要考虑更多。儿童拥有的个人装置可能不受网络保护覆盖，而且BECTA认为，重点应该放在使人人了解风险，从而有所作为方面。他们建议，这意味着需要有更多利益群体介入到电子安全政策的制定和实施中来。这些利益群体包括：

1. 班主任
2. 校长
3. 高层管理人员
4. 教师
5. 教学辅助人员
6. 青年和家长或照料人员
7. 当地政府人员
8. 互联网服务提供商（ISPs），其它电子服务提供商（ESPs），如，社交网站的公布方，正在与互联网服务提供商和其它电子服务提供商就网络安全措施紧密合作的区域性宽带集团。

BECTA认为，由于所有这些群体均有自己的想法有助于帮助学校制定政策，因此向他们进行咨询相当重要。但是，仅拥有政策是不够的，所有与儿童有关联的各方均应采取实际行动来帮助年轻人和教职员工确定并采用安全行为。在最初即欢迎所有这些群体的参予，可使所有各方感受到此类政策的相关性以及他们在落实这些政策方面所承担的责任。创建安全的ICT学习环境有若干重要因素，其中包括以下内容：

1. 对网站全面了解的基础设施
2. 责任、政策和程序
3. 有效的技术工具
4. 全面的电子安全教育
5. 为本机构中的所有人制定计划
6. 不断监控上述内容有效性的审查程序[21]。

[21] BECTA。保护网上儿童：学校校长指南（2009年）。见www.becta.org.uk/school/safety



这些均应体现在学校的现有儿童安全政策中，而不是作为仅由一个ICT团队负责的任务。不应将利用互联网或移动电话进行的欺辱视为与非在线世界中欺辱不同的事情。但是，这并不意味着技术不能成为解决方案的一部分，因而可利用技术开展以下工作：

1. 进行病毒预防并提供保护
2. 建立监控系统，以跟踪何人在何时下载了什么，使用的是哪台计算机
3. 进行过滤和内容控制，以通过学校网络尽可能减少不适当内容

显然，有关新技术的问题并不是与所有儿童有关，而且即使在问题确实出现时，也取决于使用这些技术的儿童的年龄。2008年末时，美国互联网安全技术任务组发布了其报告“加强儿童安全和在线技术”，该报告对在线性教唆、在线骚扰和欺辱以及接触不良内容等方面的许多原创文章和出版的研究进行了介绍[22]。在此报告中，作者注意到，“有一些人认为，主流媒体扩大了这些恐惧，其恐惧程度往往与年轻人所面对的风险的程度不成比例。

这带来了一种危险，即，了解的风险将被淡化，从而减少了社会解决可导致这些风险的问题的可能性，进而以未预料到的方式不经意地伤害到年轻人。”媒体报导的通过互联网进行的针对儿童的犯罪通常影射出在此领域工作的专业人员和研究人员的两极化立场。舆论一会儿摆向认为有可能歪曲了儿童所面临威胁的意见，一会儿又摆向认为威胁被远远低估的意见。

[22] ISTTF（2008年）强化儿童安全和在线技术：互联网安全技术任务组向美国各州总检察长提交的有关社交问题的最后报告。哈佛大学：伯克曼互联网与社会研究中心。

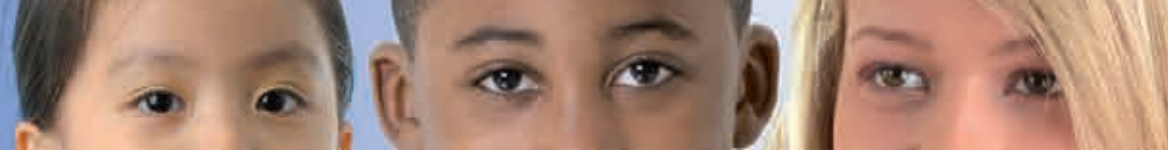
但是，人们普遍关注的是，以互联网为媒介的技术可能会导致一些儿童脆弱不堪，而教育者以及家长和监护人对此负有责任。令人惊诧的是，我们几乎不了解儿童如何就成为牺牲品，以及那些促成适应力的因素是什么。使儿童成为牺牲品的方式可包括：

1. 儿童教唆或诱惑
2. 接触不良或非法资料
3. 接触可能导致年轻人有害行为的媒介
4. 网上欺辱

以下表格介绍了考虑风险的有利方式[23]：

	商业性	进攻性	与性相关的内容	价值取向
内容（儿童作为接受方）	广告 垃圾信息 赞助方 个人信息	粗暴/充满仇恨的内容	色情或不受欢迎的性内容	持有偏见，种族主义或听取了误导信息或劝告
接触（儿童作为参与方）	跟踪/收集个人信息	受到欺辱、骚扰或追踪	与陌生人见面，或受到陌生人的诱惑	自我伤害或不受欢迎的劝告
行为（儿童作为行为方）	非法， 下载， 黑客， 赌博， 金融诈骗或 恐怖主义	欺辱或骚扰他人	产生并上传不适当资料	提供误导信息/意见

[23] 欧盟儿童在线项目制作的表格，在Byron Review 的第1.3段提及。



网上教唆或色诱

就色情教唆或诱惑而言，我们对加害过程有了更深刻的了解，其部分的原因是这项研究主要涉及儿童自身。

这项研究的资料大多来自新罕布什尔大学“伤害儿童犯罪研究中心（CCRC）”的两项研究（YISS-1和YISS-2），其中包括在2000至2005年期间对国内10-17岁互联网用户抽样进行的电话访谈。

国际青年咨询委员会的全球在线调查也提到这一问题[24, 25, 26]。

这些研究人员最近提出，互联网引起的性犯罪表明，互联网上的幼童猥亵者利用欺骗和暴力攻击儿童的老套印象，在很大程度上是不准确的[27]。

美国的这一研究表明，大多数起于互联网的性犯罪都涉及成年男子，他们利用互联网接触和引诱未成年人发生性接触。

罪犯利用即时消息、电子邮件和聊天室等互联网通信方式，与受害者会面并发展亲昵关系。

他们的做法表明，在绝大多数情况下，受害者知道他们在与成年人进行在线交谈。

迄今为止，儿童成为受虐对象被作为焦点问题，但忽视了青年人创建的各类网上社会和文化天地。

然而，儿童和青少年在成为成人互联网花样翻新手法的目标的同时，也在积极参与创建自己的网络文化。

新罕布什尔大学的研究强调指出，正是互联网的这些方面会给那些利用新技术从事某种行为的年轻人带来风险。

尽管大多数青年似乎是在**冒险**（尤其是年龄较大的男童），但绝大多数儿童似乎并未**遇到危险**。[28]

然而，向陌生人发送个人信息（如姓名、电话号码、照片）或与他们在线谈论性问题的年轻人，可能受到更为恣肆的性诱惑，包括实际或企图的网下接触。

在开展YISS-1和2研究的五年当中，性诱惑案件的总量呈下降趋势，但在少数民族青年和那些家境不富裕的青年当中，尚未看到这一趋势。

作者认为，主要可以用互联网利用率在过去5年上升来解释上述骚扰增加的情况。

---

[24] Finkelhor, D.、Mitchell, K.和Wolak, J。网络侵害：国家青年报告。（NCMEC 6-00-020）。Alexandria, VA：国家失踪和受虐儿童中心。2000年。

[25] Wolak, J.、Mitchell, K.和Finkelhor, D。网络侵害：5年后的情况（NCMEC 07-06-025）；Alexandria, VA：国家失踪和受虐儿童中心。2006年。

[26] http://www.virtualglobaltaskforce.com/iyac_charter_supp.pdf

[27] Wolak, J.、Finkelhor, D.、Mitchell, K.J.和Ybarra, M.L.网上“猎食者”及其猎物。《美国心理学家杂志》第63期(2)，2008年，111-128页。

[28] OPTEM。为儿童提供更安全的互联网。对29个欧洲中心城市的定性研究。布鲁塞尔：欧盟委员会。2007年。

然而在2005年，年轻人报告受明目张胆招揽的可能性是正常值的1.7倍，即使对人口和互联网的使用和特点的变化进行调整后依然如此。

身为女性、使用聊天室、使用移动互联网、与最初在网上结识的人交谈、向在网上初识的人发送个人信息并在网下受到身体或性虐待者，被认为这种放肆揽客行为的危害对象。

在第二次调查当中，有4%（65例）的人报称，他们在过去一年中在网上收到过发送自己色情照片的要求，但只有一人真正满足了这一要求。

非洲裔美国女性、与网络关系密切、从事网上性行为并在网下受到性或身体虐待者，面临被索要色情照片的风险。

值得注意的是，在朋友聚会上，当青少年与网上结识、给自己发送过色情照片并试图或实际进行了某种形式的离线接触的成年人联系时，较有可能被索要照片[29]。

第一次调查显示，性诱惑似乎与抑郁表现[30]相关。

报称自己有严重类抑郁症状的年轻人收到有害网上性诱惑的可能性，是抑郁症状轻微或无症状者的3.5倍，而且有抑郁症状者报告因诱惑事件而感到抑郁的可能性要高出一倍。

一般来说，抑郁症更常见于更小年龄者，即那些受到强烈诱惑或通过其家庭以外的计算机受到诱惑的青少年[31]。

瑞典的最近一项研究，对收到色情聚会或离线接触要求的16岁孩子的数量进行了观察。

在7,449名受访者当中，46%的女孩声称，她们收到过成年人的这类要求。

几位收访者报称，通过互联网或其它渠道收到过这类要求。

男孩的相应数字为16%。这些要求包括让青少年在网络摄像头前脱光衣服，或观看成人在镜头前的手淫。

该研究涉及的青少年对这种事情习以为常，称在使用聊天网站时会不断出现。

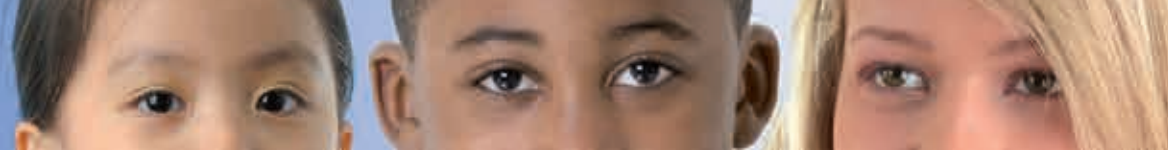
所描述的诱惑企图都毫无掩饰，成年人从聊天对话一开始就要求得到性服务。

该研究审议了警方关于利用新技术对儿童实施犯罪的报告，这些报告的犯罪当中有一半是在网上实施的，其中以索要照片或通过网络摄像头的接触最为普遍。

[29] Mitchell, K.J.、Finkelhor, D.和Wolak, J.“青少年互联网用户面临最严重的网络色诱”，美国《预防医学》杂志，2007年第32期(6)S32-S37。

[30] Ybarra, M.L.、Leaf, P.J.和Diener-West, M.“报告的青少年抑郁症候学和有害互联网色情诱惑的性别差异”，《医学互联网研究杂志》2001年第6期(1) 9-18。

[31] Mitchell, K.J.、Finkelhor, D.和Wolak, J.“青年网上色情诱惑的风险因素及影响”，《美国医学会杂志》2001年第285期(23) 3011-3014。



报告的其它犯罪是在网下实施的，但最初的联系是通过互联网建立的。

一半网下犯罪的受害者在见面时知道，会面会导致性行为。

其它犯罪则完全是在见面性质完全出乎受害者预料的情况下发生的。[32]

最近的瑞典色情教唆或诱惑受害人讲述的情况，对新罕布什尔大学的研究结果既有肯定又有否定。

瑞典一宗涉及100多位女孩子的大案表明，她们明白自己要见一个男人，以便让他与自己发生性关系。

同时，没有一个女孩承认自己完全了解这样做的后果。

肇事者从聊天当中发现女孩们的弱点，使他能够乘虚而入，利用她们满足其性欲。

这些弱点从感到孤独到萌生轻生念头，种类繁多。事实上，这些女孩主动去见肇事者并不能使她们成为情愿的主体。[33]

显然，教唆网上接触的数量庞大，青少年也报告有这类事件发生，而所有儿童都了解这一点。

从在线和离线犯罪案件的情况看，很明显，向青少年索要照片或从事网络摄像的性行为，往往标志着性虐待的开始。

近年来，有关社会网络可能置儿童于危险之中的行为，越来越多地受到关注。

我们在研究互联网给予青少年陷入有问题行为的机会时，将进一步讨论这个问题，但值得注意的是，在YISS-2之中，16%的儿童承认在过去一年中使用过博客。

博客里包括互联网用户创建的资料，并具有一些与社会网站相同的品质。

但是据调查发现，青少年和女孩是最常见的博客，而博客比其他年轻人更易于在网上发布个人信息[34]。

但是，博客们并不比他人更轻易地与网上结识但从未谋面的人拉关系。

不与他人搭讪的博客不会增加受到色情诱惑的风险，而且公布个人信息本身也不会增加他们面临的风险。

不过，无论是否与他人形成互动，博客面临更高的受到网上骚扰的风险。

---

32 Brottsförebyggande Rädet。Vuxnas sexualla kontakter med barn via Internet。[成年人通过互联网与儿童的性接触] 报告2007:11。Brottsförebyggande Rådet。2007年。斯德哥尔摩。

33 Wagner, K：Alexandramannen. Förlags AB Weinco。Västra Frölunda. 2008年。

34 Mitchell, K.J.、Wolak, J.和Finkelhor, D。“博客是否将青少年置于网上色情诱惑和骚扰的危险之中？”对儿童的虐待与忽视，32, 2008, 277-294。

“英国儿童上网调查”也说明，对生活不甚满意但又经常熟练使用互联网的青少年，会将互联网作为一种沟通环境而更加珍惜，因而导致更具风险的行为[35]。

实践和经验可以突显那些需要改变的因素，以便于我们向那些受到网上诱惑和网下性虐待的儿童提供帮助。

我们了解到，网上诱惑比网下更快捷，而且可以隐姓埋名：儿童能够与他们的网上“朋友”更快地建立信任，而且交流的内容也较少受限，违法者还不会遇到“现实”世界中的时间或接近儿童方面的困难。

通常，罪犯会尽可能充分了解受害人的情况；确定发现孩子真实身份的风险和可能性；了解孩子的社会网络；可能向孩子提供有关他们自己的假信息：如假照片和在足够安全的情况下与儿童建立某种“关系”或施加控制，使他们能够在网下与孩子见面[36]。

瑞典负责治疗受到性和身体虐待儿童的BUP Elefanten儿童和青少年精神病科，正在研究对网上和网下受利用儿童和青少年有效的治疗方法。

该项目自2006年迄今一直在进行当中，其中包括对100多名青年、治疗专家、警察，检察官和社会工作者的采访。

这些年轻人受到多种虐待，如性骚扰、网络摄像头前的性行为、将其照片上传至互联网、网上接触到网下虐待和儿童的网上性交易[37]。

对这些访谈资料的分析表明，这些年轻人可划分为三个描述性类别：

1 受骗而陷入意想不到的境地者；

2 冒险以满足情感需要和寻求关注者；

3 自暴自弃者，即进行性交易并在知情的情况下介入性乱关系者。

最后一类人不愿自己被视为“受害者”，相反认为自己具有控制能力。

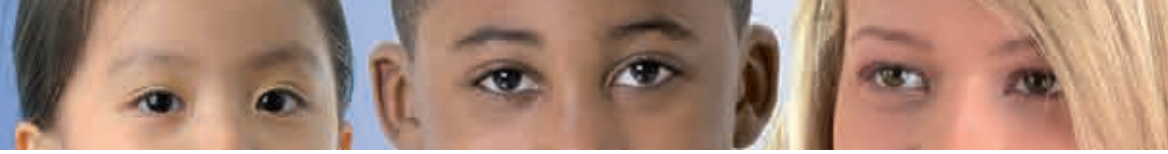
这些临床调查结果表明，很多这类儿童拒绝他人提供帮助，然而医生决不能放弃这些孩子，而要努力与他们保持联系，直到他们感到已为接受帮助或干预方法做好了准备。

受到色诱的儿童成为受虐形象的主体，打压他们的主要手段之一是迫使他们保持沉默。

[35] Livingstone, S.和Helsper, E.J.互联网上交流的风险。网下社会心理学因素在青少年易受网上风险当中的作用。《信息、通讯与社会》杂志，2007年第10期(5)，618-643。

[36] Palmer, T.《只需轻轻点击》。伦敦：Barnardos。2004年。

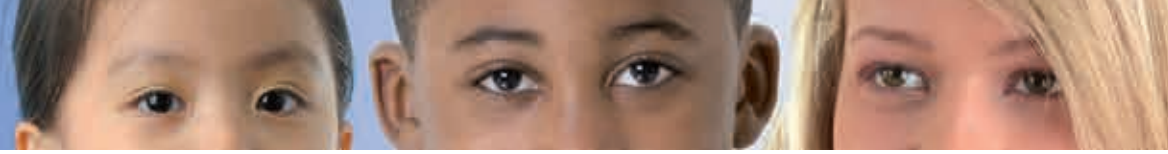
[37] Quayle, E., Lööf, L. & Palmer, T.（2008年）。《网上的儿童色情和性剥削》。曼谷：ECPAT International。



这种沉默是由两个因素促成的：青少年确信他们要见的人是朋友，而且他们不希望承认自己在网上进行了那种性质的交谈。

第一点暗示出青少年界定和确定友谊的方式，而后一点涉及前面提到的内容，即青少年网上交流受到的限制要少得多。

互联网几乎可将青少年带到世界的任何角落，但在这一过程中，他们可能面临潜在的危险



评估有问题的网上资料

虽然假设互联网出现之前不存在色情或性化资料是幼稚的，但有理由说明互联网使方便获取的性资料得以泛滥。

互联网的易获性、交互性和匿名性，正是使人们更有可能接触暴力和色情资料的因素。

SAFT的研究表明，34%的儿童偶然或故意地浏览过暴力网站[38]。

新罕布什尔大学的研究重点提出了青少年偶然接触有害的网上色情资料的问题，但承认现有对他们接触有害的网上色情资料的研究主要是在学生和年轻的成年人，而不是在青少年当中进行的，而且主要涉及自愿而非偶然的接触。

有人假设，不同类型的青少年卷入网上性虐待和性剥削关系的情况说明，冒险者和自暴自弃的青少年也可能访问为迎合寻求性伴侣的成人而设的聊天网站，但支持这一论点的研究结果寥寥无几。

YISS-1的调查表明，在数据采集的前一年中，经常上网的孩子当中有1/4看到过有害的色情照片，73%的这类接触是在青少年网上搜索或冲浪时发生的，而且这种情况大多发生在家中，而不是在学校。

这些作者还讨论了那些维持这类性接触的编程技术，使青少年难以脱身。在令人痛心的事件中，有三分之一出现了这种“捉老鼠”的情况。

大多数接触了这类资料的儿童，并不认为这种接触特别令人不安。

然而，作者强调这种接触，特别是有害的接触，可能会影响对性和互联网的态度，影响青少年的安全和团体意识。

根据YISS-2的调查结果，有害接触的情况有增无减，这在10-12岁的儿童、16至17岁的男孩以及白人和非西班牙裔青年当中尤其明显[39]。

对澳大利亚青年（16-17岁）的研究显示，四分之三的人偶然浏览过色情网站，而38%的男孩和2%的女孩有意访问过这些网站[40]。

这项研究的结论是，儿童接触色情的两个特点可以反映成人这方面的情况。

[38] SAFT，安全意识事实工具。布鲁塞尔：欧盟委员会。2007年6月5日评估自：http://ec.europa.eu/information_society/activities/sip/projects/awareness/closed_projects/saft/index_en.htm。

[39] Mitchell, K.J.、Wolak, J.和Finkelhor, D.“青少年报告的互联网色情诱惑、骚扰和有害色情接触的趋势”，《青少年健康杂志》2007年第40期，116-126。

[40] Flood, M.“澳大利亚青年的色情接触”，《社会学杂志》2007年第43期，45-60。

首先，男性更可能成为X级电影和色情网站的追求者和频繁消费者。

其次，任何年龄的互联网用户都很难免接触到有害的性暴露资料。

这方面的一个例子涉及到一些电脑游戏，其中可能含有很多的色情内容。虽然这些游戏可能被定为“成人级”，但无可避免地享有青少年的高度参与。

还必须认识到，这种接触并不为新技术所独有，而也可能发生在电视等传统媒体，如当儿童收看节目时，可能正是性爱和色情节目的播出时间。

这其中的一个重要因素可能涉及接触的可控性，而且偶然接触和有意接触的影响也有所不同。

人们还发现，很多未成年人对在使用互联网过程中偶然看到的节目内容感到惊讶[41]。

意外或部分接触上述资料可能是一个重要问题，因此有人提出[42]：“较新的技术（包括视频，也包括互联网和移动通信）使内容的收视受到扭曲。

人们可能是从看到的一系列预告片，而不是整个故事情节去了解内容的。“编辑语境”一直是重要的内容监管准则（如BBFC、Ofcom），但可能很难将它变为同样适用于新媒体的准则。

有关儿童意外接触网上色情的研究显示，意外及无语境的内容尤其令人不安。这对监管机构提出了挑战。”

不过，目前尚未对年轻人使用色情作品进行广泛的研究，多数是根据自我报告进行的，这其中的差别很可能在于那些现行的社会规范会对青少年做出强制规定。

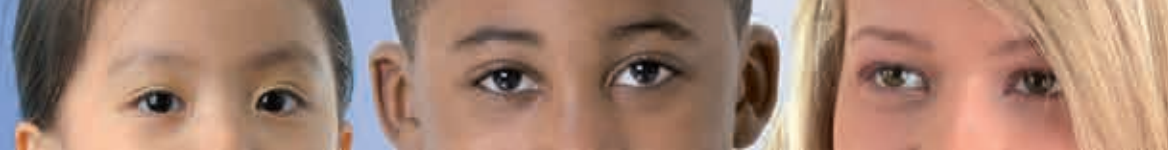
我们有充分的理由认为，许多儿童和青少年都会声称他们只是偶遇色情内容，因为他们认为说明自己主动在互联网上寻找这类内容是不妥当的。

瑞典的抽样调查显示，在18岁的青年当中，65%的男孩每月都会观看色情内容，而相比之下，只有5%的女孩这样做。值得注意的是，在研究涉及的孩子当中，只有7%的男孩和31%女孩表示从没看过色情内容[43]。

[41] Fug, O.C.“拯救孩子：对信息社会的儿童的保护和音响媒体服务局”《消费者政策杂志》2008年第31期，45-61。

[42] Livingstone, S.和Hargrave, A.M.“有害于儿童？从有关媒体影响的实证研究中获得结论。U. Carlsson (ed) 的监管、意识及赋能。数字时代的年轻人和媒体内容。”Göttenborg：Nordicom. 2006年。

[43] Mossige, S.、Ainsaar, M. 和 Svedin, C.G.“波罗的海地区关于青少年性行为的研究”18/07号NOVA报告，93-111。



许多青年接触到网上色情资料，而且我们也很清楚，并非所有的接触都是偶然发生或有害的。

令人担心的是，接触异常或暴力色情可能对一些年轻人的信仰和态度产生影响，但只会在较低程度上影响到极少数个人的行为。

这越来越被视为一种潜在的公共健康问题，而且看来，通过互联网这类几乎不受监管媒体的接触造成的后果，无疑值得进一步研究[44]。

有问题的机会

新技术带来的又一个风险涉及媒体自身，而在人们看来，赋予青少年参与机会的方式值得关注。

这或许可被称为通过互联网和移动电话技术的自我伤害行为，不过这一说法看上去会令人不可思议，因为它在很大程度上涉及与日俱增的在线内容生成能力。

有证据表明，11-16岁儿童的手机拥有率高于成人，拥有自己手机的儿童占总数的76%。[45]

[44] Perrin, P.C., Madanat, H.N., Barnes, M.D., Corolan, A., Clark, R.B., Ivins等人。卫生教育在确定色情为公共卫生问题方面的作用：具有国际影响的本地和国家战略。《宣传与教育》杂志，2008年第15期，11-18。

[45] Child-Wise Monitor (2002年)。2007年6月18日访问：http://www.childwise.co.uk/monitor.htm

通过2004年对英国Teesside地区1,340名中学生的调查发现，86%的学生拥有了移动电话（女生为89.7%，男为82.3%）。[46]

这项研究将移动电话的用途仅限于语音呼叫和文本，但有证据说明，移动电话越来越可能用于其它形式的通信。

然而**英国儿童上网**研究显示，目前正在出现多样化趋势，38%的青年人拥有移动电话、17%拥有数字电视和8%购置了游戏机，而且都有上网能力。

在许多年轻人看来，移动电话既是重要的通信工具，也是联系和参与广泛社会的途径。

在2007年对29个欧洲国家进行的OPTEM定性研究表明，绝大多数的孩子拥有移动电话。

然而，令人愈发感到关切的是，这类技术参与也可能含有针对他人的甚至危及自身的行为。

自拍的图像或电影可被视为诱惑过程的一部分，违法者利用它套取孩子们的裸体或性行为照片。

图像通常被用来使孩子们相信，孩子和成人间的性接触是无害的，以打消他们对网下性行为和有偿地与成人见面的顾虑。

成为目标的孩子的脆弱性源于孤独、受到胁迫或与家长持续冲突等多种原因。在施虐者的照片发出后，牵涉其中的青少年会认为自己是虐待事件的同谋。

新罕布什尔大学的研究小组通过研究1,504名医疗工作者所存的病案，对伤害问题作了研究，以观察哪类上报的有问题经历与新技术相关。

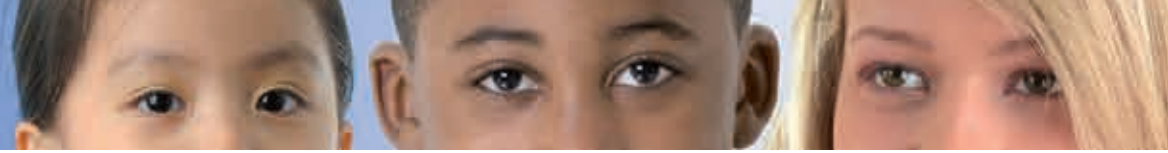
他们发现了青年和成人客户报告的十一类有问题的经历，如沉迷网络、色情、不忠行为、性剥削与虐待、游戏、赌博和角色游戏、骚扰、孤立自闭措施、欺诈、盗窃与欺骗、失败的网上关系、具有不利影响的网站和危险的不当用途[47]。

进一步的分析研究了哪些有问题的经历被视为主要或次要问题[48]。

青年和成人用户更有可能面对沉迷网络、收看成人色情、儿童色情、性剥削犯罪、游戏、赌博和角色游戏的问题。

其它同样可能出现的与互联网相关的问题有自闭措施、性剥削侵害、骚扰犯罪和网上不忠行为。

[46] Madell, D.和Muncer, S.“刚从海边回来就煲电话粥？”英国青少年对移动电话和互联网的态度和体验。《网络心理学和行为》2004年第7期(3)，359-367。
[47] Mitchell, K.J.、Becker-Blease, K.A.和Finkelhor, D.“临床工作中遇到的有问题的互联网体验案例集”。《专业心理学：研究与实践》2005年第36期(5)，498-409。
[48] Mitchell, K.J.和Wells, M.“有问题的互联网体验：寻求精神医疗保健者提出的主要或次要问题?”《社会科学和医学》2007年第65期，1136-1141。



据认为，与游戏、赌博和角色游戏相关的问题是青少年当中出现最多的问题，其发生率是其它问题的1.7倍，而发生网上欺诈或者欺骗侵害的可能性为四倍。

受到性剥削的青少年与其它具有与互联网相关问题的青少年相比，更可能被诊断患有创伤后应激障碍症（PTSD）。

胁迫

我们曾经提道，不应认为网上胁迫与网下行为有什么区别。人们有时称网上或通过移动电话的胁迫为“网络胁迫”，但这并不总能使大家了解实情。胁迫就是胁迫，无论它以哪种方式出现。

英国的《拜伦研究述评》提出，“网络胁迫是指通过电子方式从事的诸如发送威胁性文本消息、公布有关一些人的不光彩行为和传送关于某人的难堪照片或视频的胁迫行为。”

网上或通过移动电话的胁迫既可以是当面胁迫的延伸，也可以是对网下事件的报复。网上或通过移动电话的胁迫可让人不胜其烦并极具杀伤力，因为它传播广泛、破坏性强，而且以电子方式散布的内容能够随时重新炒作，使受胁迫者更难以最终了结；其中可能含有诽谤性视图和伤人感情的语言；其内容24小时随时可取，以电子方式进行的胁迫从不间断，受害者就连在家中这类否则“安全”的去处也无隐秘可言；而且可以对个人信息做手脚、对视图偷梁换柱，然后传送给他人。

更有甚者，这一切可以匿名进行[49]。

这种胁迫可能包括戏弄和极具攻击性的行为。新罕布什尔大学的研究指出，性骚扰和胁迫这类非法行为之间在很大程度上是重叠的。

德国最近的一项研究从受害者的角度，对聊天室的敲诈行为进行了观察[50]。

他们发现的不同类型的胁迫包括骚扰、虐待、侮辱、讥笑和敲诈。

这样胁迫频繁发生，并且通常以孩子为对象。

重要的一点是，该项研究还显示，学校和聊天室的受侵害体验之间存在联系。

在学校被胁迫的青少年也可能有在聊天室受侵害的经历。

这些孩子有可能被认为不那么讨人喜欢、缺少自信，并可能受到家长溺爱。

这项研究还显示，这些孩子经常在受害者和加害者之间转换角色，而这可以被解释为“反击”或“撒气”。

来到聊天室的受害儿童还报称，他们时常出没于危险的网址，实际上将自己置于更易于受到伤害的地位。

研究表明，与重大的校园胁迫相比，访问聊天室过程中出现的主要聊天胁迫常常表现出社会上造假手法（例如提供虚假年龄或性别信息）。

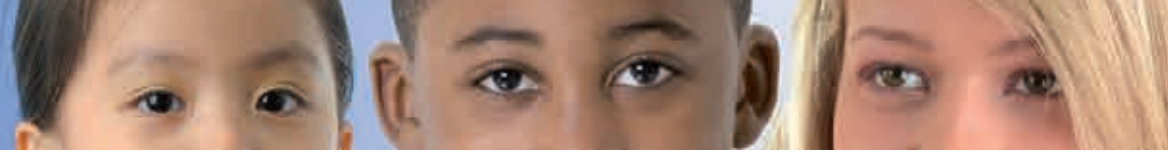
对美国儿童的研究得出的结论是：

1. 互联网的常客一般都有受到“网上胁迫”的经历
2. 网上和校园胁迫的形式相似，并且这两种环境下的体验相互重叠
3. 虽然某些电子通信方法和设备具有较高的“网上胁迫”风险，但它们仅仅是工具，不是有害行为的诱因
4. 网上胁迫独立于校园胁迫，但与忧虑的增加相关
5. 青少年很少告诉成人其受到网上胁迫的体验，而且未能充分利用通信技术提供的工具防患于未然[51]。

[49] Byron, T. (2008)。“让数字世界中的孩子们更安全”，《拜伦研究述评》。请访问：http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf

[50] Katzer, C.、Fetchenhauer, D.和Belschak, F. Cyberbullying：谁是受害者？“互联网聊天室受害者和校园受害者的比较”，《媒体心理学》杂志，2009年，第21期(1)：25-36。

[51] JUVONEN, J.和Gross, G.F.，“校园空间的延伸？ - 网络空间的胁迫体验”，《学校健康杂志》，2008年第78期(9)，496 – 505。



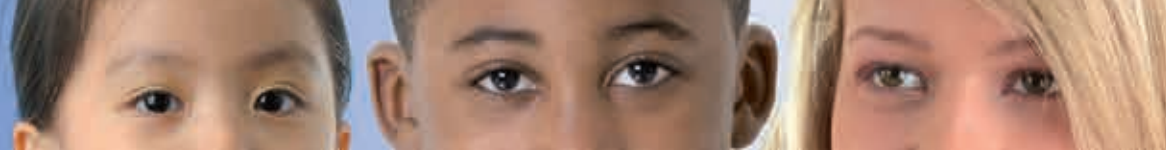
4. 家长、监护人和教育者指南

这些安全提示源于对收集数据的分析和现有的研究资料。本文的这一部分旨在从一个方便位置，向家长，监护人和教育者提供一份指南，帮助他们教会子女获得安全、积极和可贵的网上体验。

父母、监护人和教育者必须考虑不同站点的确切性质，其子女对风险的了解，以及在决定哪种环境适合孩子之前，考虑到家长化解风险的可能性。

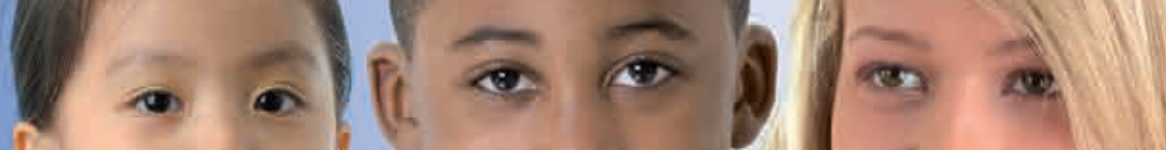
互联网在赋予青少年学会自立和认识事物能力方面潜力巨大。教授正面和负责任的网上行为是主要目标。

家长、监护人和教育者			
	#	考虑的重点	说明
个人电脑的安全可靠性	1.	将电脑置于共用房间	至关重要的一点是，要将电脑置于共用房间，而且家长尤其要在孩子使用互联网时在场。如果您不能在场，可考虑采用技术工具等其它方式，密切注意孩子的网上活动。在有多台电脑的大家庭，你可以做出要求孩子同时待在同一房间等可行规定，但要记住，随着孩子年纪的增长，他们无论如何也应享受一定的隐私权。随着越来越多的儿童拥有笔记本电脑和无线网络在家庭的普及，维持这类规定的难度也会增加。
	2.	安装防火墙和反病毒软件	确保您的电脑安装了防火墙和反病毒软件，并不断得到更新。向孩子传授基本的互联网安全知识。
规则	3.	通过有关使用互联网和个人装置的内部规则，并对隐私权、年龄不宜站点、胁迫行为和陌生人的危险给予特别关注	一旦孩子开始独立使用互联网，讨论制定一份经认可的规则表，其中应包括孩子使用互联网的时间和方式。
	4.	经认可的手机使用规则	一旦孩子开始独立使用移动手机，讨论制定一份经认可的规则表，其中应包括孩子是否可利用手机上网、上网的频率、可利用手机购买或下载的资料、应对不宜内容的方式和支出额度。



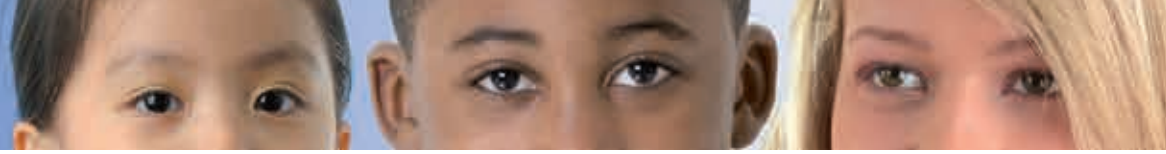
家长、监护人和教育者			
	#	考虑的重点	说明
家长、监护人和教师的教育	5.	家长应熟悉其子女使用的互联网网站（即互联网网站提供的服务和产品）并掌握孩子的网上活动	评估孩子计划使用的站点，仔细阅读隐私政策、使用条件和行为准则（通常被称为“内部规则”）以及所有家长专用网页。还要了解网站是否监测服务页面张贴的内容，并定期审核孩子使用的网页，检查网站是否出售任何产品。
	6.	调查网上资源，更深入了解有关网上安全的信息和积极利用互联网的方式	全球每年都举行积极和安全使用互联网的宣讲活动。这可能涉及儿童、当地学校、行业和相关参与方共同努力，增进对实现积极网上体验的机会的认识。欲获得有关这些活动的最新信息，请在网上搜寻“互联网宣讲活动”+“国名”等短语。
	7.	了解儿童使用移动电话、游戏机、MP3播放机和PDA等其它个人装置的方式	目前可通过其它多种个人装置访问互联网，因而在这些环境下，也出现了类似的安全问题。

	#	考虑的重点	说明
互联网网站特点纵览	8.	考虑能否通过使用过滤和阻拦或者监控程序，为青少年安全使用互联网和个人设备提供支撑或后盾。如果您使用这类软件，请说明其用途和您将它用于孩子的原因。对链接这些程序的所有相关密码实行保密。	在使用技术工具，特别是使用监控程序时，可能出现信任和年轻人隐私权的问题。在正常情况下，家长或监护人最好能够说明其希望使用这类软件的原因，而且学校也应对此做出充分解释。
	9.	家长认可	西班牙和美国等国家的法律规定了公司或网站可在不首先征得家长同意的情况下，要求青少年提供个人信息的最低年龄限制。西班牙为14岁，美国为13岁。其它国家则认为妥善的做法是，征得家长同意后再要求青少年提供个人数据。许多为青少年服务的站点会先征得家长同意才允许新用户加入。请查验您的孩子希望加入或已是其成员的网站对这一认可提出的要求。
	10.	对使用信用卡和其它支付方式的控制	对利用陆线或移动电话购买虚拟物品实施控制。如果允许儿童利用陆线或移动电话任意购买虚拟物品，这会是太大的诱惑。您同样需要确保您的信用卡和借记卡的安全，不要泄漏个人密码。
	11.	确保对网上购买产品和服务的年龄验证	通常，购买商品是不核实年龄的，然而已有一些可在销售点核实年龄的系统上市。在任何情况下都应仔细监测您的孩子的网上消费。



	#	考虑的重点	说明
	12.	了解互联网站是否进行规管	确保互联网网站对网上交谈进行规管，最好同时采用自动过滤器和人工监测方式。网站是否对它公布的所有照片和视频进行检查？
	13.	拦阻对不宜内容或服务的访问	技术工具可以帮助您阻止用户访问不良网站，例如访问放任无管束内容或讨论上网的站点，也能阻止通过手机获得不良服务或内容。
	14.	检验合同的灵活性	检查删除帐户的方法 - 即使这将导致丧失订费。如果该服务不允许删除帐户，就考虑不使用它，或阻止对它的访问。将无法删除的情况告知地方当局。
	15.	检查业务范围	分析内容提供商的政策及其遵守情况，检查提供的内容和具体服务，并认识到技术的局限性（如可能无法对广告做此明确界定）。
	16.	监测广告宣传并举报不当广告	关注广告，并向您的当地广告管理机构举报以下类型的广告： 1. 因过度简化复杂问题而出现误导的。 2. 教唆儿童与陌生人交谈或访问危险网址的。 3. 向他人，特别是儿童，展示自己使用危险物品或靠近危险品的。 4. 鼓动进行不安全的效仿或从事危险举动的。 5. 鼓动胁迫行为的。 6. 给儿童造成精神损害和恐惧的。 7. 鼓励不良饮食习惯的。 8. 利用儿童的信任。

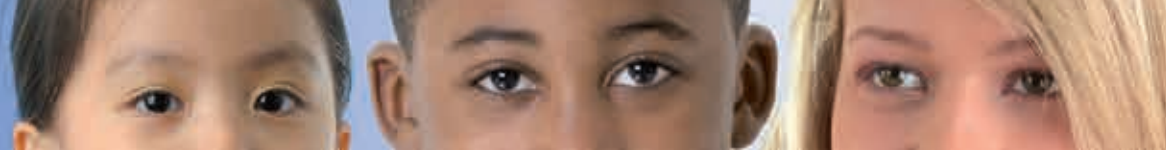
	#	考虑的重点	说明
儿童教育	17.	教育您的孩子	教育和培养媒介素养至关重要。对虚拟世界导则和规则作出说明。儿童可能会遵守指导原则，并会时常提醒他人也这样去做。教育你的孩子不要回复粗鲁留言，避免网上的色情交谈。教导他们不要打开任何与他人聊天时收到的附件或链接，因为其中可能含有有害内容。
	18.	告诉孩子决不与网上邂逅的人会面	如果儿童与只在网上联系的陌生人会面，就可能面临真正的危险。家长应只鼓励孩子利用互联网网站与其网下的朋友交流，不与他们从未见过的人联系。上网的人不一定使用真实身份。然而，如果确实在网上建立了牢固的友谊，而且您的孩子希望安排一次会面，为了不让孩子只身或无人陪伴地冒险前往，您可以告诉他您愿陪他一起去，或保证有可信任的成年人一同前往，并确保首次会面将在一个照明良好、人员聚集的公开场合进行。
	19.	防止孩子向他人泄漏可识别的个人信息	帮助你的孩子了解什么样的信息应予保密，并说明儿童应只公开自己和对方乐于让他人看到的信息。提醒您的孩子，信息一旦上网是无法收回的。
	20.	确保孩子明白网上发布照片，包括使用网络摄像头意味着什么	告诉您的孩子，照片可以暴露大量的个人信息。儿童不应未经家长、监护人或负责照顾他们的成年人的允许，使用网络摄像机或上传任何内容。要求孩子不上网公布自己或其朋友的带有清晰可辨细节的照片，如路牌、汽车车牌或其运动衫上的校名。
	21.	告诫儿童不要向陌生人表露情感	儿童不应直接与陌生人进行网上交流。要告诉他们，访问同一个网站的所有人都可看到他们所写的内容，而且流氓地痞往往寻找表示希望结交新朋友的孩子下手。



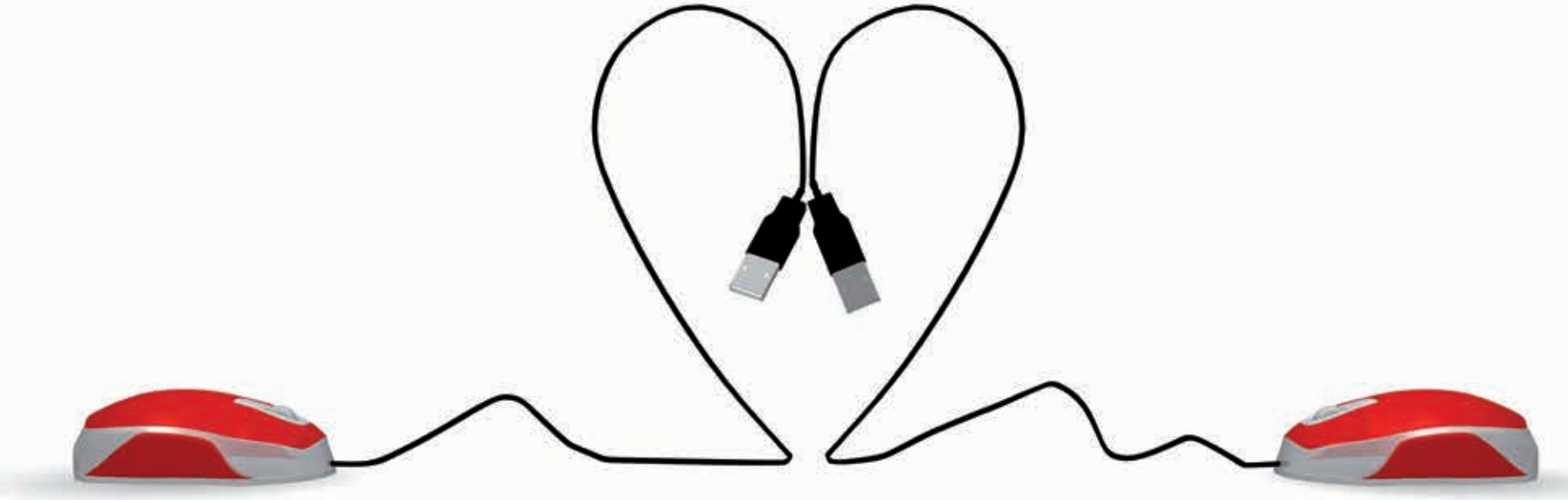
	#	考虑的重点	说明
互连网站安全使用回顾	22.	检查您孩子的网页或简介	定期检查您孩子的网页。登录查看您孩子帐户的历史情况并在必要时将您孩子聊天的模式变更为您认为合适的模式。设计良好的互联网站为您提供了深层次介入您孩子上网经验的机会。如果您孩子拒绝遵守网站的规则，您可以考虑联系网站，要求将您孩子的网页和简介删除。值得一提的是，这应该可以向您孩子突出规则重要性以及违反规则所带来的后果这一讯息。
	23.	确保孩子遵守互联网站的年龄限制	如果您孩子的年龄小于互联网站所推荐的年龄，不要让他们使用这些网站。父母不能依赖服务提供商来阻止年龄不足的小孩登录网站，记住这一点是非常重要的。
	24.	确保孩子没有使用全名	尽可能让孩子使用化名，不要使用他们的真实姓名或部分使用真实姓名。应仔细选择化名，以免引起不适当的注意。不能允许您孩子公布其朋友的全名或任何可用来确定其朋友身份的其它信息，如他们所居住街道的名称、上学的地点、电话号码、运动俱乐部等。
交流	25.	与您孩子交流其上网经验	定期与您的女子交流他们上网时浏览的站点以及交谈的对象。鼓励您孩子说出互联网上令他们感到不适或受到危胁的情况。当您孩子感到不安或觉得可疑时，提醒他们立即停止正在做的事情。确保他们理解向您告知情况并不是制造麻烦。而您作为父母和成人，当您孩子与您分享其体验时不应反应过度。不管他们告诉了您什么，都要保持冷静，全面了解情况后再采取行动。表扬您孩子对您的信任。确保孩子能够举报虐待者。

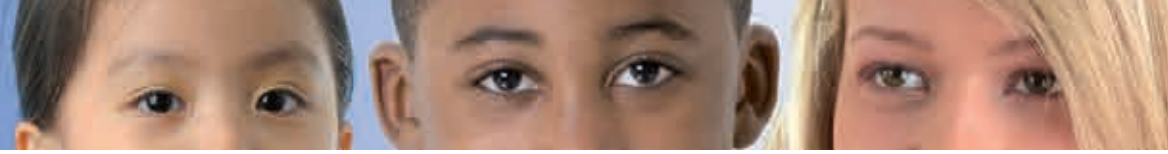
教育部门[52]			
		考虑的重点	说明
作为儿童保护战略一部分的安全和防护	1.	要采取全机构参与的措施，负起电子安全（e-safety）的责任。	即使学校不允许在学校内使用某种技术，学校也必须告诉学生在使用该技术时如何做到行为理智得体并说明其中的风险。
	2.	制定一项可接受的使用政策（AUP）。	这些政策应详细规定职员、学生和所有网络用户（包括父母在内）可以和不可以使用ICT设施的方式。
规则和政策	3.	通过在线和本地主管部门提供AUP的样本。	规则必须量身定制，以适应您单位的具体情况。
	4	将AUP与其它学校政策联系起来。	这些应包括反恐吓等政策以及关于版权和剽窃的导则。
	5.	单一的联系人。	指定一位高层管理团队成员负责保护工作，同时也作为所有电子安全问题的统一联系人。
	6.	需要领导。	班主任应在校长的支持下，带头将协商一致的电子安全政策落实到行动上。
做到宽宏包容	7.	让年轻人保持觉悟。	确保您负责的年轻人了解潜在的风险，并且无论何时何地上网，都能做到行为安全、举止负责。
	8.	培养适应能力。	允许年轻人在没有成人监管且没有技术保护时，制定其自己的保护战略。
	9.	鼓励揭露恶行和承担责任。	帮助年轻人了解他们无需为他人强加于他们的行为负责，但如果他们在网络上有不正当的行为，学校将进行处罚。

[52] BECTA（2008年）保护在线儿童。针对学校领导的指南可查阅：www.becta.org.uk/schools/safety



		考虑的重点	说明
技术解决方案	10.	检查行动。	确保定期回顾并更新技术措施和解决方案，以保持电子安全计划的有效性。
互联网安全政策	11.	教师的互联网安全政策培训。	在互联网安全方面为教师提供培训，帮助并支持实现儿童网上安全。
	12.	教育学生绝不在与他人交流时公布个人信息。	告诉学生，在与网络上的陌生人交流时，绝不应该公布个人信息（如全名、地址、电子邮件、电话号码、所在学校等）。
	13.	要求学生只搜索具体的信息。	要求学生搜索具体的信息，而不是在互联网上随意的“冲浪”并用目录格式记录所使用过站点的URL。
	14.	在向学生们发送链接之前预先检查或测试互联网站。	在建议学生浏览某个网站前，确保自己先去访问。在请学生访问URL之前，提前将网站放入书签。





5. 结论

信息通信技术-或ICT-改变了现代的生活方式，向我们提供了实时通信，跨越国界且几乎没有限制的信息接入以及一系列广泛的创新服务。

与此同时，它们也为钻空子和滥用提供了新的机会。如果没有适当的保护，作为互联网频繁使用者之一的儿童就面临着接触到暴力、色情和其它不良图像的风险。

如果不致力于创建一个安全的网络环境，我们将辜负我们的孩子。尽管人们越来越多地认识到不安全使用ICT带来的风险，仍然有许多工作需要开展。

因此，父母和教育工作者必须能够确定什么内容可以适当且安全地供其孩子使用，以及如何负责任地使用ICT。

携起手来，父母、教育部门和儿童可以享受ICT带来的好处，同时将可能对儿童带来的风险降到最低限度。

我们希望，这些指导原则将通过提供清晰全面的信息，说明儿童在线保护问题、儿童可能遇到的风险以及父母和教育部门保护儿童并帮助他们了解如何在多方受益于ICT的同时，将潜在风险降至最低。

参考文件和补充阅读的原始资料

Children’s Online Privacy Protection Act (COPPA) http://www.coppa.org/coppa.htm

Cyberpeace Initiative, 可查阅 http://www.smwipm.cyberpeaceinitiative. org

Cyril. A. Wantland, Subhas C. Gupta, Scott A. Klein, Safety considerations for current and future VR applications，可查阅http://www. webmed.com/i-med/mi/safety.html（最后一次访问时间为2008年9月4日）。

‘Are ads on children’s social networking sites harmless child’s play or virtual insanity?’, The Independent，2008年6月2日，可查阅http://www.independent.co.uk/news/media/are-ads-on-childrens-social-networking-sites-harmless-childs-play-or-virtual-insanity-837993.html（最后一次访问时间为2008年6月11日）。

‘Children’s social-networking sites: set your little monsters loose online’, Telegraph.co.uk，2007年11月17日，可查阅http://www.telegraph. co.uk/connected/main.jhtml?xml=/ connected/2007/11/17/dlchildren17.xml（最后一次访问时间为2008年6月10日）。

CBC News, Cyber-bullying, 2005，可查阅http://www.cbc.ca/news/background/bullying/cyber_bullying.html（最后一次访问时间为2008年9月4日）。

Child Exploitation and Online Protection Centre (CEOP): Think You Know，可查阅http://www.thinkuknow.co.uk/parents/gaming/ bad.aspx（最后一次访问时间为2008年9月4日）。

Children, Adolescents, and Television, American Academy of Pediatrics, Pediatrics, Vol. 107, No. 2，2001年2月，可查阅http://aappolicy.aappublications.org/cgi/content/full/pediatrics;107/2/423（最后一次访问时间为2008年9月10日）。

Cyber-bullying: Developing policy to direct responses that are equitable and effective in addressing this special form of bullying, Canadian Journal of Educational Administration and Policy, Issue n. 57，2006年12月18日，可查阅http://www.umanitoba.ca/publications/cjeap/articles/brown_jackson_cassidy.html（最后一次访问时间为2008年9月2日）。

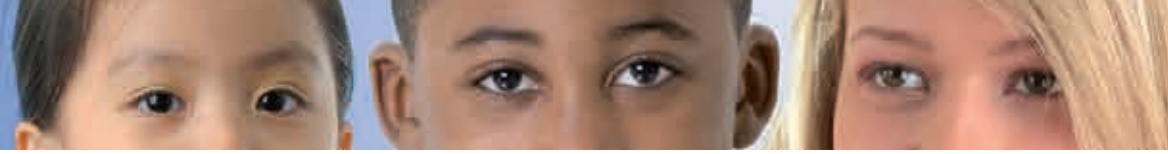
eModeration, Virtual World and MMOG Moderation: Five techniques for creating safer environments for children，2008年5月，可查阅http://www.emoderation.com/news/press-release-virtual-world-and-mmog-whitepaper（最后一次访问时间为2008年7月22日）。

Entertainment & Leisure Software Publishers Association (ELSPA), Unlimited learning – Computer and video games in the learning landscape，可查阅 http://www.elspa.com/assets/files/u/unlimitedlearningtheroleofcomputerandvideogamesint_344.pdf（最后一次访问时间为2008年8月26日）。

ENISA, Children on virtual worlds - What parents should know，2008年9月，可查阅http://www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf

Gauntlett, David and Lizzie Jackson, Virtual worlds – Users and producers, Case study: Adventure Rock, Communication and Media Research Institute (CAMRI), University of Westminster, UK，可查阅http://www.childreninvirtualworlds.org.uk/pdfs/Gauntlett_and_Jackson_May_2008.pdf

Home Office, Home office task force on child protection on the internet – Good practice guidelines for the providers of social



networking and other user interactive services 2008，2008年，可查阅http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance?view=Binary（最后一次访问时间为2008年6月16日）。

Home Office, Good practice guidance for the providers of social networking and other user interactive services 2008，可查阅http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance（最后一次访问时间为2008年9月12日）。

Home Office, Good Practice Guidance for the Moderation of Interactive Services for Children，可查阅http://police.homeoffice.gov.uk/publications/operational-policing/moderation-document-final.pdf（最后一次访问时间为2008年9月12日）。

http://disney.go.com/fairies/pixiehollow/comingSoon.html（最后一次访问时间为2008年8月26日）。

http://www.redherring.com/Home/2418（最后一次访问时间为2008年7月10日）。

Internet Watch Foundation: Protection Online http://www.iwf.org.uk/public/page.36.htm

Keith, Stuart, ‘SpongeBob is the real threat to our children online’, The Guardian，2008年4月10日，可查阅http://www.guardian.co.uk/technology/2008/apr/10/games.news（最后一次访问时间为2008年7月10日）。

Kirriemuir J., A Survey of the Use of Computer and Video Games in Classrooms, Nesta Futurelab Series，2002年，可查阅http://ccgi.goldingweb.plus.com/blog/wp-content/Games_Review1.pdf（最后一次访问时间为2008年9月2日）。

Kramer, Staci D., Disney Acquires Club Penguin; $350 Million Cash, Possible $350 Million Earnout, paidContent.org，2007年8月1日，可查阅http://www.paidcontent.org/entry/419-disney-acquires-club-penguin-in-deal-values-at-700-million-to-be-brande/（最后一次访问时间为2008年7月10日）。

Mediashift, Virtual Worlds for Children Entwined with Real World，可查阅http://www.pbs.org/mediashift/2007/06/your_take_roundupvirtual_world.html（最后一次访问时间为2008年8月28日）。

Microsoft, How to help your children’ use social networking Web sites more safely，2006年11月9日，可查阅http://www.microsoft.com/protect/family/activities/social.mspx（最后一次访问时间为2008年6月11日）。

NSPCC: Children and the Internet http://www.nspcc.org.uk/whatwedo/mediacentre/mediabriefings/policy/children_and_the_internet_media_briefing_wda49338.html

The Children’s Charity: Net Smart Rules http://www.nch.org.uk/information/index.php?i=135

Virtual Worlds Management, Disney.com Launches Games and Virtual Worlds Portal; Mobile Widgets，2008年8月14日，可查阅http://www.virtualworldsnews.com/2008/08/disneycom-launc.html（最后一次访问时间为2008年8月26日）。

Virtual Worlds Management, Virtual Worlds Managements Youth Worlds Analysis，2008年8月22日，可查阅http://www.virtualworldsmanagement.com/2008/youthworlds0808.html（最后一次访问时间为2008年8月25日）。

Virtual Worlds News, Virtual World 125,000 Children Fight Obesity in Whyville，可查阅http://www.virtualworldsnews.com/2007/06/virtual_world_h.htm（最后一次访问时间为2008年9月4日）。

大使计划，用于培训培训师-各种网站都有关于这一点的好的实例。http://www.saferinternet.at/tipps/fuer-eltern/

教育素材。有许多优秀的资源可用于传递电子安全讯息。以下清单并不详尽，更进一步的来源可查阅http://www.saferinternet.org/ww/en/pub/insafe/resources.cfm

http://www.digizen.org/cyberbullying/film.aspx是几个网站用来应对恐吓的一个优秀资源。

http://www.internetsanscrainte.fr/le-coin-des-juniors/dessin-anime-du-mois Vinz et Lou – 几个旨在提高电子安全意识的法国卡通片。

http://www.cybereth-ics.info/cyethics2/page.php?pageID=25&mpath=/35提供了一系列针对教师的最好提示。

http://www.easy4.it/content/category/13/59/104/是来自意大利网站，旨在为教师提供支持的素材。

http://www.teachtoday.eu/en/Lesson-Plans.aspx该网站提供了一系列计划用于学校的授课计划。该网站正在更新，将很快提供更多的信息。

http://dechica.com是保加利亚网站为儿童开发的一个提高意识的游戏。

www.microsoft.com/cze/athome/bezpecnyinternet -由微软发布的如何更安全的使用互联网的flash版娱乐手册。2009年“安全互联网日”期间进行了宣传。

www.tietoturvakoulu.fi – 更加安全地使用互联网以及“做个精明的上网者”的测试。

接受视频采访的拉脱维亚名流介绍了他们对在线恐吓的看法和个人经历。语言：拉脱维亚语
更多的采访：
电视采访2（电视明星）：

http://www.youtube.com/watch?v=QttMrRABnR0&feature=related-电视采访3（舞蹈演员）：

http://www.youtube.com/watch?v=3cPRlhQDJAg&feature=related-电视采访4（拉力赛车手）：
http://www.youtube.com/watch?v=PodsmBjrE6Y&feature=related-电视采访5（政客）：
http://www.youtube.com/watch?v=4_xrUvDQaIY&feature=related-电视采访6（歌手）：
http://www.youtube.com/watch?v=usqpmAHjHQ4

www.tietoturvakoulu.fi.父母可以在网站上利用该在线测试测试自己在媒体教育方面的知识。语言：芬兰语和瑞典语。

http://www.medieradet.se/Bestall--Ladda-ner/filmrummet瑞典媒体委员会网站的一部分，专用于动态图像资料
语言：瑞典语以及部分英语。

http://www.lse.ac.uk/collections/EUKidsOnline/ European Research on Cultural, Contextual and Risk Issues in Children's Safe Use of the Internet and New Media

http://www.nortononlineliving.com/提供了几个国家发展趋势的概况。

http://www.pewinternet.org/Pew提供了一系列广泛的互联网使用和相关技术的报告。设在美国的这家公司认为，历史说明源于美国的发展趋势会最终向欧洲转移。

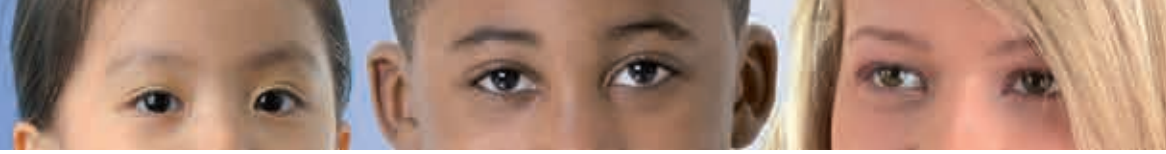
http://www.unh.edu/ccrc/是David Finkelhor关于逮捕互联网捕食者发展趋势的研究，该研究表明，没有确凿的证据说明互联网造就了更多捕食者。

http://www.webwise.ie/article.aspx?id=10611，爱尔兰网站开展的研究。

http://www.childnet-int.org/youngpeople/

www.kidsmart.org.uk

www.chatdanger.com



附录1

B内置保护

PC和Mac在其操作系统和每个最新的系统（Windows Vista和Mac Leopard）中，都内置了父母控制（Parental Control）功能。如果您在考虑升级操作系统，该控制开关可能为您节省额外的监控软件费用。

要使用您计算机的控制功能，首先为您每一个孩子建立个人用户帐户。如果您对如何操作没有把握，请查阅您计算机的用户指南。

苹果Mac用户：下一步，在Apple menu中选择System Preferences，然后点击Accounts。对于每一个孩子的帐户，点击Parental Controls，然后您将看到一个您可以限制或监控的类别清单（Mail, Safari等）。

如果您在运行Leopard，可以记录即时传讯（IM）的通话并为孩子指定通过e-mail 或iChat通话的对象。您也可以限制屏幕显示时间。例如，您可以将电脑设定为在晚上8点自动让您的孩子退出登录。

Windows用户：可通过控制面板（Control Panel）打开Parental Control。查找用户帐号（User Accounts）和家庭安全控制面板（Family Safety Control Panel）。在Windows Vista中，您可以选择网页限制，也可以选择获得您孩子使用计算机的报告。您可指定某个禁用时间段并阻止令人讨厌的电脑游戏和软件。

无论您使用哪一种操作系统，绝大多数浏览器（Safari，Firefox等）都有自动历史记录功能，显示访问过的站点。如果您不熟悉的话，请查阅您的用户手册，学习如何检查历史记录。如果您的电脑上有多个浏览器，确保对它们进行逐个检查。请注意：孩子可以学会如何删除历史记录，以掩盖他们的上网踪迹。所以如果您发现历史记录被别人删除了，请向孩子询问。

您还需要更多的帮吗？苹果（Mac）和微软（Windows）在其网站上都有在线指导和详细信息-只要在Google中输入“parental controls”和“Apple”或“Microsoft”，就可以找到这些信息。

请记住，您给予孩子的任何保护都不可能是百分之百的。您需要尽可能与孩子交流并与其讨论儿童在线保护问题。

附录2

网上缩略语解密

缩写和代码词能够加快即时讯息和文本的传递，但它们也给人们的话语加了一层掩饰！请您做好准备，以下是一些常用的短语：

ADIH: Another day in hell
（又是糟糕的一天）

A/S/L: Age, sex, location
（年龄，性别，地点）

BTDT: Been there done that
（去过，做过）

CULTR: See you later
（再见）

GTFO: Get the f-ck out
（表示惊讶）

H8: Hate（不喜欢）

ILY或143或<3: I love you
（我爱你）

JK或J/K: Just kidding
（逗你玩儿）

KWIM: Know what I mean?
（明白？）

LLS: Laughing like sh-t
（滥笑）

LMIRL: Let’s meet in real life
（我们真正见面吧）

LYLAS (B): Love you like a sister (brother)
（爱你就像老鼠爱大米）

NIFOC: Naked in front of computer （在电脑前裸体）

PAW或PIR或P911: Parents are watching或Parent in room (drop the subject)
（父母在看或父母在房间，换话题）

POS: Parent over shoulder
（父母就在我身后，也可用来表示骂人的“piece of sh-t”）

Pr0n：故意拼错的“色情”一词

STFU: Shut the f-ck up （表示惊讶，而不是训斥的说法）

TMI: Too much information
（太多信息）

TTFN: Ta ta, for now （再见）

WTF: What the f-ck?
（怎么回事）

来源：http://www.parenting.com/article/Mom/Relationships/How-to-Spy-on-Your-Child-Online/3

图片鸣谢: www.shutterstock.com, Violaine Martin/ITU, Ahone Ayeh Njume-Ebong/ITU

国际电信联盟
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int/cop

瑞士印刷
2011年，日内瓦

本指南得到以下机构的协助：