DOI:10.13718/j.cnki.jsjy.2018.05.015

# 澳大利亚OESC保护中小学生上网安全的途径研究

高婷婷,周 琴

(西南大学 教育学部,重庆 400715)

**摘 要:**随着网络技术的发展和社交软件使用的低龄化,发生在中小学校的网络欺凌现象越来越普遍。澳大利亚政府高度关注该问题,专门成立网络安全专员办公室(OESC),用以支持和推动中小学生网络安全措施的实施。具体而言:(1)提供安全的网络使用指导,引导中小学生养成网络安全行为习惯;(2)为学校和家庭提供相关的教育资源,培养中小学生的网络安全意识和能力;(3)对网络服务供应商设立监管机制,确保中小学生网络安全措施的顺利实施。

**关键词:**澳大利亚;OESC;中小学生;网络欺凌;网络安全

**中图分类号:**G611 **文献标识码:**A **文章编号:**2095-8129(2018)05-0111-07

网络欺凌指的是通过电子媒介对他人造成有意的、重复的伤害[1]。随着信息通信技术和社交媒体的快速发展,网络欺凌问题越来越突出,并且对中小学生造成了严重的精神创伤。2006年和2007年澳大利亚分别以709名高中生和652名11至17岁的中小学生为调查对象,进行了一项关于网络欺凌现象的调查。结果表明,有20%~36%的学生曾经遭遇过网络欺凌[2]。2009年,澳大利亚以7 500名中小学生为对象开展了一项包括欺凌者和受害者在内的网络欺凌现象的匿名调查。结果表明,大约有5%的小学生和8%的中学生曾经遭遇过网络欺凌[3]。2014年,澳大利亚政府的又一项调查表明,青少年之间网络欺凌的受害率从之前的6%上升到40%以上[4]。澳大利亚政府高度重视发生在中小学生之间的网络欺凌现象,因此,通过设立网络安全专员办公室①(Office of the eSafety Commissioner,简称OESC)来支持和推动中小学生网络安全措施的实施。

## 一、提供网络使用指导,引导中小学生的网络行为

一方面,OESC提供安全使用网络与技术的信息资源;另一方面,OESC也为中小学生提供全面防范与应对网络欺凌的策略。

### (一)安全使用网络与技术

在安全使用网络与技术方面,OESC努力使中小学生理解个人隐私的重要性、知道如何保护个人隐私以及了解如何管理个人数字声誉并建立良好的网络形象。此外,OESC还提供了如何安全

① 2015年7月1日,儿童网络安全专员办公室(Office of the Children's eSafety Commissioner,简称OCeSC)正式成立;2017年2月,为了扩大办公室的职能,改名为网络安全专员办公室(Office of the eSafety Commissioner,简称OESC)。

**收稿日期:**2017-12-19

**作者简介:**高婷婷,西南大学教育学部硕士研究生。

周琴,教育学博士,西南大学教育学部副教授。

**基金项目:**中国博士后科学基金资助"基于MOOC平台的教师专业学习共同体构建研究"(2016M602618),项目负责人:周琴;西南大学2016年度基本科研重点项目"互联网+时代教师网络学习共同体构建研究"(SWU1609120),项目负责人:周琴。

使用主流社交媒体、搜索引擎以及网络游戏等相关信息。

1. 个人信息的重要性及保护

《1988 年隐私法》(*The Privacy Act* 1988)将个人信息定义为关于一个确定的(合理识别的)人的信息或意见,不管是否真实。通俗地讲,个人信息即是使个人能够被识别的任何信息或信息的组合,可能包括全名、家庭住址、电话号码、学校名称、生日、电子邮件地址、用户名和密码以及银行明细等。OESC 严格遵守《1988 年隐私法》中对个人隐私义务的规定,并且明确指出保护个人隐私信息的重要性。

通常情况下,许多在线服务都要求用户提供一些个人信息,主要分为 4 类:第 1 类是购物类活动,需要验证购买者的身份,以处理付款或交付货物事宜;第 2 类是订阅或注册类活动,通常最低要求是提供用户名称或身份(ID),再加上电子邮件地址,有时还需要用户的年龄、性别、地址、照片和个人喜好等;第 3 类是竞赛、奖品和奖励类活动,通常要求用户提供广泛的个人数据,然而这些信息常常被营销人员用来作为宣传其产品和服务的工具;第 4 类是在线游戏和虚拟世界类活动,这些可能需要用户注册才能使用。以上 4 类在线活动极易造成个人信息的泄露,一旦在线泄露个人信息,极有可能遭遇垃圾邮件、诈骗、身份被盗用等事件。

因此,在线保护个人信息需要做到以下几点:(1)只在安全网站上披露财务信息,即浏览以"https://"开头的地址和多媒体设备且屏幕底部有"已锁定"挂锁符号,表示数据正在加密的网址;(2)如果对网站的合法性有任何疑问,要致电相关部门查询;(3)银行机构绝不会向个人请求发送其用户名或密码的电子邮件,如果用户收到该类电子邮件,不要回复,也不要点击其任何链接;(4)在线购买产品、在线参加竞赛或注册服务、在线填写电子邮件时,要仔细阅读用户协议和隐私政策,并强调禁止私人信息用于营销目的;(5)谨慎创建和保存密码[5]。

2. 数字声誉的重要性和保护

了解个人信息的在线使用情况以及保护个人信息和数字声誉(digital reputation)①非常重要。因为上传照片、博客帖子,社交网络互动等在线活动是当事人将自己展现给他人,不但关乎当事人的数字声誉,而且与当事人的人际关系,甚至工作机会息息相关。保护个人数字声誉需要从 3 个方面入手:(1)仔细审查发送到社交媒体上的任何内容;(2)注意使用网络文明用语进行交流沟通;(3)将个人资料设为私人,并随时检查以确保设置未被系统更改。

**(二)防范与应对网络欺凌**

在防范与应对网络欺凌方面,OESC 主要引导中小学生认识网络欺凌现象和表现方式、识别网络欺凌行为,以及了解在遭遇网络欺凌时如何向家长和学校求助,并学习向社交媒体和 OESC 投诉的方法。

1. 识别网络欺凌行为

网络欺凌(cyberbullying)是指利用多媒体技术欺凌某个人或某个群体,旨在对他们造成社会、心理甚至身体上的伤害[6]。网络欺凌行为可能包括:辱骂性的文字和电子邮件,有害信息、图片或视频,在线模仿别人,在线排挤别人,在线羞辱别人,在线用龌龊的语言说闲话或闲聊等。

2. 向家长、学校求助

许多学校制定了详细的规章制度,包括为中小学生提供网络安全方面的支持,以及如何处理网络欺凌等问题。此外,各州教育部门的政策规定也为学生、教师、家长和广大社区提供相关信息,帮助提高网络安全意识并严厉打击多媒体技术滥用等行为。

3. 向社交媒体和 OESC 投诉

一方面,大多数社交媒体都有一个安全中心,主要包括指导用户如何安全使用网站,以及如何处理一系列有损网络安全的问题,包括网络欺凌、在线滥用和隐私泄露等。因此,一旦遭遇网络欺

① 数字声誉是由用户在在线环境中的行为以及发布的有关自己和他人的内容来定义的。

凌行为，中小学生或其监护人应该立即向社交媒体服务商举报该媒体上出现的网络欺凌内容。一经举报，社交媒体服务商应该在两天之内移除被举报的网络欺凌材料。一旦决定向某社交媒体服务投诉，中小学生或其监护人则需要提供网络欺凌材料的一些细节。例如：带有网络欺凌材料的照片、截图或网络欺凌材料出现的网站、网址等。

另一方面，如果社交媒体服务商未在两天之内移除被投诉的网络欺凌材料，中小学生或其监护人可以选择向 OESC 进行投诉。具体而言，进入 OESC 官网设置的“投诉与报告”(complaints and reporting)系统，并依次完成相应资料的填写。主要包括以下 4 个步骤：(1)向发生网络欺凌的社交媒体服务商报告网络欺凌材料的内容；(2)搜集网络欺凌材料的证据；(3)向 OESC 报告网络欺凌内容；(4)屏蔽他人[7]。

此外，一旦向 OESC 完成投诉，中小学生或其监护人还将收到电子邮件回复。其中，回复的电子邮件中还可能包含网络安全的自助策略和获取支持服务(如儿童帮助热线)的信息，以及关于如何更广泛地处理和应对网络欺凌的实用建议。需要特别注意的是，如果由于其他障碍或技术原因而无法完成在线投诉表格的填写，还可以下载投诉表格，填写完成后通过电子邮件返回至：complaints@esafety.gov.au。

## 二、提供教育资源，培养中小学生的网络安全意识和能力

OESC 通过与各行业、各州政府和非盈利网络安全组织合作，为中小学生、家长、教师和广大社区提供可扩展和可持续的网络安全教育资源，包括面向中小学生的课堂资源及其配套的课程计划、虚拟课堂、“重写你的故事”(rewrite your story)教育项目等。

### (一)学校教育资源

学校教育资源主要是为中小学生提供课堂资源。OESC 自成立以来，陆续开展虚拟课堂、“重写你的故事”教育项目，以及开发中小学课堂资源，为中小学生提供网络安全引导和教育资源。

1. 开展虚拟课堂，为中小学生普及网络欺凌的常识

OESC 积极与澳大利亚各州和领地的教育部门合作，提供一系列免费的虚拟课堂。虚拟课堂是网络安全拓展项目的子项目之一，采用网络研讨会的形式进行学习，虚拟课堂可以使各地区的学校通过虚拟网络参与到拓展项目中。网络研讨会通常约 30～40 分钟，虚拟课堂的主要对象是小学四至六年级的学生。OESC 提供给小学四至六年级学生的虚拟课堂内容主要包括：认识网络欺凌的严重危害性、如何处理网络欺凌、在线保护个人信息、文明上网等。例如：主题为“小学中高年级：尊重的交谈，我能做到”(Upper primary：Respectful chat，I can do that)的活动结合“网络智能英雄”(Cybersmart Hero)、“游戏开始”(Game On)、“网络欺凌测验”(Cyberbullying Quiz)和“50 项班级活动挑战赛”(ClassAct 50 challenge)等资源，通过演示，帮助学生认识遭遇网络欺凌时出现的情绪低落、行为极端等问题，并在严重时寻求心理帮助。OESC 还通过主题为“小学高年级：更好的互联网安全从你开始”(Upper primary：A better internet starts with you)的网络研讨会，向四至六年级的学生详细介绍如何向 OESC 报告严重网络欺凌的全过程，以及明确维护网络安全是创建尊重和包容的在线和离线的学校社区和家庭社区的重要策略。另外，虚拟课堂在 2016－2017 年度计划中增加了 4 个关键主题，即“尊重对话”(Respectful chat)、“保持在线尊重”(Keep it sweet online)、“在游戏中保持安全”(Keeping safe in the game)以及“你的品牌是什么”(What's your brand)。“2017 年更安全互联网日”(Safer Internet Day 2017)虚拟课堂吸引了来自全国所有州和领地的 32 197名学生和教师——这是 OESC 参与该国际活动以来参与者数量最多的一次。2016－2017 年度，虚拟教室这一子项目共有 66 889 参与者。

2. 开发课堂资源，提高中小学生维护网络安全的能力

OESC 参照澳大利亚中小学课程学习目标，为中小学生免费提供网络安全方面的课堂资源，其中包括游戏类、网络智能挑战系列和新的课堂资源，并开发相应的课程计划，旨在培养中小学生良

好的数字素养、正确处理网络欺凌等安全问题的意识和能力。

第一,“Zippep 马戏团”(Zippep and his circus)是通过一系列针对学前到小学二年级(5～7 岁)儿童的游戏活动,帮助儿童建立初步的网络安全观念,包括介绍适合儿童的网站、了解网络欺凌现象、学会保护个人信息和密码安全、与信任的成年人交谈、分享积极的在线经验等。该学习活动旨在鼓励儿童安全并负责任地使用在线技术,知道网络上可以信任的网站,适时展示密码和私人信息以及初步培养积极的在线社交行为。“游戏开始”(Game On)活动则是为学生提供《网络欺凌》《过度游戏》《分享密码》《免费下载》和《在线朋友》等 5 个网络安全教育视频节目,用以指导学生形成安全的网络行为和掌握初步的网络安全知识。在“游戏开始”基础上,“游戏和测验”(Games and quizzes)旨在为 6 岁以上的小学生提供现有课程计划和基于班级(class-based)的网络安全活动,通过有趣的互动游戏和测验,强化学生关于网络欺凌、网络安全、共享密码、免费下载和在线交友等 5 个方面的网络安全意识。

第二,“网络智能挑战”(Cybersmart Challenge)是免费提供给澳大利亚小学生的一系列由教师主导的课堂活动,主要由《网络智能侦探》(Cybersmart Detective)、《网络智能英雄》(Cybersmart Hero)和《网络智能永恒》(Cybersmart Forever)3 个相互补充的动画节目组成,旨在教育和指导小学生学会正确应对现实生活中的网络安全问题。“网络智能挑战”系列是针对四年级(8～10 岁)学生提供的半小时互动课堂活动动画,让学生身临其境。《网络智能侦探》节目旨在帮助学生识别在线发布的内容、向何处寻求有关网络安全问题的帮助、区分理智和危险的在线行为等。《网络智能英雄》节目旨在帮助学生识别什么是网络欺凌;遭遇网络欺凌时,应该采取什么措施;遭遇网络欺凌时,应该在何时向何处寻求帮助;遭遇网络欺凌时,如何做一个积极的旁观者。《网络智能永恒》节目旨在帮助学生学会理解数字内容或图像的安全共享;学会使用策略来保护数字内容或图像;遭遇数字内容或图像滥用时,学会寻求帮助。同时,“网络智能挑战”系列课程符合澳大利亚健康与体育(Health and Physical Education)、技术(Technologies)、一般能力(道德理解)(General Capabilities (Ethical Understandings))等学习领域的要求,相关网络安全知识会贯穿其中。

第三,“数字公民”(Digital Citizenship)指的是具有技能和知识的人积极、自信地使用数字技术参与社会活动,与他人沟通并创建和使用数字内容。负责任的数字公民应该遵循 3 个核心原则:积极参与、了解在线世界、理智选择。数字公民通过与非营利性机构、行业合作伙伴、政府合作伙伴、公司合作伙伴的合作,为澳大利亚中小学生提供健康与体育(Health and Physical Education)、公民与公民教育(Civics and Citizenship)、技术(Technologies)等领域的学习资源,并配备相应的课程计划,帮助学生了解描述个人“数字足迹”的重要性、在线保护个人隐私(密码)的安全行为、在线选择信任的人、在线识别积极和消极的社交行为。这些课程培养了学生良好的数字素养,进而有效预防和解决网络欺凌现象,维护网络安全。

3. 不断补充新的网络安全资源,拓宽中小学生网络安全知识的渠道

在 2016－2017 年度,OESC 新增加“重写你的故事”教育项目(Rewrite your story,RYS)。该项目通过 8 部真实网络欺凌事件的短片,以及提供专业人士的建议和支持,旨在增强中小学生在线行为控制能力。“重写你的故事”是一个以探索青少年遭遇网络欺凌和其他网络安全问题为重点内容的教育项目,旨在鼓励中小学生勇敢面对网络欺凌现象,为中小学生提供网络安全引导,以及帮助中小学生支持遭遇网络欺凌的朋友。

“重写你的故事”教育项目已经获得 3 个重大奖项:世界媒体艺术节通识教育金奖(Gold Award in General Education at the World Media Festival)、纽约电影节指导和教育世界铜奖(Bronze World Medal in Instruction and Education at the New York Festivals)、澳大利亚导演协会在线戏剧项目最佳指导奖(Best Direction in an Online Drama Project at the Australian Directors Guild Awards)。该项目还提供了关于如何及何时向 OESC 报告严重网络欺凌的基本信息。

“重写你的故事”教育项目的课程计划旨在探讨网络欺凌的主题、影响和寻求帮助的途径,重点

是探索网络欺凌对自己、他人、家庭和学校社区的影响。具体而言，通过一系列高质量的短片、互动问答、班级讨论等活动，鼓励中小学生思考、讨论关于网络欺凌行为和其他负面在线行为，进而探索现实生活中应对网络欺凌的策略，帮助中小学生找到“重写故事”的途径。同时，该课程计划符合澳大利亚课程要求的一些能力目标，包括信息和通信技术、道德行为和个人社交能力。

基于“重写你的故事”教育项目的网络资源，OESC 提出其课程目标为：(1)对严重的网络欺凌行为进行界定；(2)在技术使用的背景下理解社会和道德礼仪的概念；(3)在使用技术时，谨慎分析所作出的决策和行动对自己、他人、家庭和学校社区的影响；(4)熟悉“重写你的故事”网站上的相关信息，重点包括如何举报严重的网络欺凌行为。此外，OESC 也提出其他课程活动(见表 1)。

**表 1 “重写你的故事”教育项目课堂活动**

| 活动内容 | 活动主题重点 | 活动时间 | 活动所需资源 |
| --- | --- | --- | --- |
| 活动一：找到严重网络欺凌的所有信息 | 中小学生如何通过真实的网络欺凌经历寻求帮助 | 20～45 分钟 | 网络欺凌互动测验；“重写你的故事”视频 |
| 活动二：如何“重写你的故事” | 识别负面的在线行为并决定可接受的行为 | 1 分 41 秒的视频；10～45 分钟的课堂讨论 | “重写你的故事”视频 |

另外，OESC 还增加了新的网络安全资源：重新设计和更新的“网络智能英雄”教育资源——一项交互式的多媒体课堂活动；借助“50 项课堂活动挑战赛”(Class Act 50 Challenge)活动让学生在网络欺凌的场景中变成主动积极的旁观者；其他系列日常任务的课堂资源，帮助中小学生思考建立彼此尊重关系的重要性，并知道如何在网上获得支持。

**(二)家庭教育资源**

2016 年 6 月，OESC 对澳大利亚 2 360 名家长进行了一项关于 8～17 岁中小学生使用互联网情况的调查。结果表明，有 60％的家长表示他们的孩子面临网上的风险，其中，29％是网络欺凌，38％的家长需要有关网络安全信息来应对网络欺凌等危险的发生[8]。这项调查显示，在网络异常发达的时代，中小学生总是面临着各种各样的网络安全问题，其中网络欺凌现象是最常见的。网络欺凌并不仅仅发生在学校，也可以在家庭中出现。所以，为了引导中小学生注意网络安全、丰富在线体验，“家长在线安全指南”(Parent's guide to online safety)为所有年龄段学生的父母提供了一些关键的网络安全实用信息和建议。具体包括：首先，向社交媒体服务商举报在该媒体出现的网络欺凌材料，大多数社交媒体服务商在他们的网站上都有举报的链接；其次，提供网络欺凌材料中的细节，简单的办法就是拍一张照片或对网页截图、复制网址；如果社交媒体服务商未及时处理投诉，就向 OESC 举报网络欺凌问题；再次，屏蔽此人，建议家长帮助屏蔽欺凌孩子的人或解除其好友关系，这样在移除网络欺凌材料的同时可以避免中小学生受到二次伤害。

需要特别注意的是，如果中小学生遭遇网络欺凌，并表现出很苦恼或显示其行为、情绪方面有很大异常时，家长要向“儿童帮助热线”(Kids Helpline)和“网络引导空间”(eHeadspace)寻求专业支持。“儿童帮助热线”专门为儿童提供免费、保密的在线及电话心理辅导，一天 24 小时全天候服务。“网络引导空间”为 12～25 岁的年轻人及其家人提供一个保密、免费和安全的空间，可以通过面谈、电子邮件或电话等方式与专业人士进行交流。

**(三)社会教育资源**

社会教育资源主要是以拓展项目的形式展开，而拓展项目则是由专门的培训师(OESC 的高级教育顾问)免费提供给澳大利亚有志于教师职业的群体且有专业发展需求的教师群体和其他与中小学生教育密切相关的社会群体，旨在增强教师在保证中小学生上网安全方面的意识、知识和技能等。主要有以下几种：

1. 职前教师项目(pre-service teacher program)

为了确保有志成为教师的学生能够在未来的工作中充分了解学校网络安全问题，拓展教育项目内容，将为其在高等教育的最后一年提供免费的短期培训，旨在为职前教师提供知识、技能和信心，以此来教育他们帮助中小学生应对网络安全问题。职前教师项目通过“演讲＋个别辅导＋网络

研讨会”的方式进行培训。首先是 1 小时的演讲，主要向参与者提供网络安全知识和网络欺凌材料，帮助学习者将这些知识融入进专业教学活动当中，讨论包括网络安全问题、个人声誉管理和在线沟通等问题，此外，还会额外增加 1 个半小时的时间进行讨论和提问；其次是 1 小时的个别辅导，向参与者提供有关网络安全的教学实践，讨论将网络安全战略纳入到课堂和课程实践中的策略，以及开展基于情境的学习活动；最后是增加网络研讨会的互动环节，即与其中一位培训师进行 1 小时的有关网络安全问题的深入讨论。

2. 教师必备专业发展项目(teacher essentials PD program)

教师必备专业发展项目包含虚拟课堂计划的各个方面，该项目由 3 个 50 分钟的网络研讨会和一个 30 分钟的测验组成。

首先，要参加教师专业发展项目，必须提前注册。3 个网络研讨会分别在 1 年中不同的时间举行，需要选择适合的时间参加。其次，只有参加并完成 3 个网络研讨会的培训，才可以进行 30 分钟的测验来完成该项目。但需要注意的是，如果教师仅参加 3 个网络研讨会中的一个，将不提供专业发展证书，但可作为支持教师专业发展的证明。最后，所有教师和相关人员完成该项目后将收到一个包括关键学习内容和证书的信息图。新南威尔士州和澳大利亚首都领地的教师也将通过新南威尔士州教育标准局/教师资格指数(NESA / TQI)获得 3 小时的专业发展认证。

3. 社区演示(community presentations)

网络安全拓展项目还为那些与中小学生工作相关和互动的群体(如心理健康和社会工作者、家长和其他监护人团体、企业集团、执法团体等)提供量身定制的演示会。这些演示会均由 OESC 的网络安全专家免费提供。演示会长度在 1～2 小时，是基于现实场景的活动，以处理和应对中小学生网络安全方面的问题为目的。社区演示介绍了 OESC 快速删除严重网络欺凌材料的能力，详细描述当前网络技术的趋势，并提供有针对性的安全建议，以保证中小学生更安全和更愉快的在线体验。

## 三、对网络服务供应商设立监管机制，保证中小学生上网安全

澳大利亚联邦政府专门针对社交媒体服务供应商设立了监管机制。《2015 年加强网络安全法》制订了一个社交媒体服务分级方案，用于从社交媒体服务中删除针对澳大利亚 18 岁以下中小学生的网络欺凌材料。该法案规定澳大利亚中小学生可以访问的所有社交媒体服务都将有一个投诉管理系统和充分禁止网络欺凌材料的使用条款以及与 OESC 的联络点，以便提交用户认为没有得到充分处理的投诉。此外，根据社交媒体服务供应商的服务情况划分为 1 级和 2 级两个大类，并受到不同级别的监督和监管：1 级社交媒体服务供应商是以合作为前提的；2 级社交媒体服务供应商则可能收到具有法律约束力的通知和受到民事处罚。

### (一)1 级社交媒体服务供应商的监管

社交媒体服务供应商可主动向网络安全专员申请成为 1 级社交媒体服务。申请必须以书面形式提交，并附加或链接表明该服务符合《2015 年加强网络安全法》第 21 节所规定的基本在线安全要求的信息。1 级社交媒体服务供应商有很多权限：首先，1 级社交媒体服务供应商可以参照其自行设定的使用条款来界定网络欺凌并受理投诉，而不是依据《2015 年加强网络安全法》；其次，1 级社交媒体服务供应商意味着网络欺凌受害者可以及时要求从涉及的社交媒体服务供应商处移除相关内容，以尽量减少对受害人的潜在伤害，也减轻网络安全专员和 OESC 的工作负担。

### (二)2 级社交媒体服务供应商的监管

《2015 年加强网络安全法》规定，根据网络安全专员的建议，通信部可直接宣布某社交媒体服务供应商为 2 级，或者某社交媒体服务供应商未在网络安全专员发出邀请的规定时间内(28 天)主动申请成为 1 级社交媒体服务供应商，那么网络安全专员就会向通信部建议将其降为 2 级社交媒体服务供应商。此外，如果 1 级社交媒体服务供应商在 1 年内经常出现不能及时处理网络欺凌材料的投诉，网络安全专员就会认为其不符合基本的在线安全要求，那么就会取消其 1 级社交媒体服

务供应商的身份，并向通讯部建议将其降为2级社交媒体服务供应商。

定为2级社交媒体服务供应商是一项社交媒体服务民事处罚措施，对社交媒体服务供应商具有法律约束力，是对其采取的民事处罚，即如果2级社交媒体服务供应商没有及时处理有关网络欺凌材料的投诉，那么，一旦网络安全专员接到投诉且核实材料后，就会强制要求2级社交媒体服务供应商在48小时内删除该内容，否则，网络安全专员有权执行民事处罚措施，如罚款或下达正式警告，并在OESC官网上进行通告。

综上所述，澳大利亚政府通过OESC这一独立机构，提供3种保护中小学生上网安全的途径：一是为中小学生提供安全的网络使用指导，引导中小学生形成安全的网络行为；二是为学校和家庭提供相关的教育资源，培养中小学生网络安全意识和能力；三是为社交媒体服务供应商设立监管机制，保证中小学生上网安全。《2015年加强网络安全法》中设立了社交媒体服务分类方案，也是投诉系统的关键组成部分，目的在于给中小学生提供一个快速移除潜在的、有害的网络欺凌材料的途径。

澳大利亚政府反网络欺凌行动为我国应对网络欺凌问题提供了以下启示：重视安全使用网络与技术的教育；建立中小学生防范与应对网络欺凌的引导机制；关注经历网络欺凌的中小学生的心理健康；重视面向中小学和家庭的网络安全教育资源的培训；重视学校、家庭和社交媒体服务供应商之间的合作；重视完善网络欺凌监管体制和法律制度的建设。

**参考文献：**


[1] PATCHIN J W, HINDUJA S. Bullies move beyond the schoolyard: apreliminary look at cyberbullying[J]. Youth Violence & Juvenile Justice, 2006, 4(2): 148-169.

[2] FLEMING M J, GREENTREE S, COCOTTI-MULLER D, et al. Safety in cyberspace adolescents' safety and exposure online[J]. Youth & Society, 2006, 38(2): 135-154.

[3] DOOLEY J J, CROSS D, HEARN L, et al. Review of existing Australian and international cyber-safety research[R]. Perth: Child Health promotion Research Centre, Edith Cowan University, 2009.

[4] KATZ I, KEELEY M, SPEARS B, et al. Research on youth exposure to, and management of, cyberbullying incidents in Australia: synthesis report[R]. Sydney: Social Policy Research Centre, UNSW Australia, 2014.

[5] Australian Government: Office of the Children's eSafety Commissioner. How can I protect my personal information[EB/OL]. (2017-11-12)[2017-02-20]. https://esafety.gov.au/esafety-information/esafety-issues/protecting-personal-information.

[6] Australian Government: Office of the Children's eSafety Commissioner. Parent's guide to online safety[EB/OL]. (2017-02-20)[2017-11-19]. https://esafety.gov.au/about-the-office/resource-centre/brochure-parents-guide-to-online-safety.

[7] Australian Government: Office of the Children's eSafety Commissioner. What if the cyberbullying material is still there? [EB/OL]. (2017-02-20)[2017-11-21]. https://esafety.gov.au/esafety-information/esafety-issues/cyberbullying.

[8] Australian Government: Office of the Children's eSafety Commissioner. Kids Online: Parent views and information needs[EB/OL]. (2017-02-21)[2017-12-09]. https://esafety.gov.au/education-resources/iparent/kids-online-infographic.


## Approaches to Online Safety Protection for Primary and Secondary School Students in OESC in Australia


GAO Tingting, ZHOU Qin

(*Faculty of Education, Southwest University, Chongqing* 400715, *China*)



**Abstract**: With the development of network technology and the increasing number of younger users of social software, cyberbullying in primary and secondary schools is becoming more and more common. The Australian Government pays close attention to this issue and sets up the Office of the eSafety Commissioner to guide the protection of students' online safety through three channels. Firstly, they provide instructions on safe use of network to guide students' online behaviors. Secondly, they provide relevant educational resources for schools and families to train students' awareness and ability of online safety. Thirdly, they establish a supervision mechanism for network service providers to protect students' online safety.



**Key words**: Australia; OESC; primary and secondary students; cyberbullying; online safety

责任编辑　邱香华