

## 网络霸凌政策

阅读本政策时应结合 [《反霸凌政策》](#)、[《行为政策》](#)、[《安全措施和儿童保护政策》](#)（包括防范措施）以及 [《行为准则》](#)。

学校认识到，当有合理理由相信儿童正在遭受或可能遭受重大伤害时，应将霸凌事件视为一项儿童保护问题。

### 网络霸凌

网络霸凌可以被定义为“利用电子通信，尤其是移动电话和互联网霸凌某人，一般是通过发送具有恐吓或威胁性质的信息：儿童和成人可能不愿意承认自己是网络霸凌的受害者”。网络霸凌可能具有多种不同形式：威胁和恐吓、骚扰或“网络跟踪”（例如，反复发送令人厌恶的短信或即时消息）、发送性短信（例如，主要通过手机发送和接收色情信息）、中伤/诽谤、排挤/同伴拒绝、假冒、未经授权发布私人信息/图像、“用恶毒语言攻击和抹黑他人”（滥用互联网煽动或冒犯网络上的其他人）和激进化。网络霸凌可能是面对面欺凌的延伸，技术为霸凌者提供了另一个骚扰霸凌目标的途径。

然而，网络霸凌与其他形式的霸凌之间存在若干重要的不同点：

- 进一步实施一种更为极端的个人空间入侵。可在任何时间实施网络霸凌，且之前被认为安全的个人空间也遭到侵犯。
- 霸凌者可能会匿名。这对受害者来说可能非常痛苦。
- 霸凌者可以迅速对更多的受众施加影响，因此网络霸凌的规模和范围可能大于其他形式的霸凌行为。
- 霸凌者知道所发布的信息处于公众的目光之下，这在极大程度上增加了对受害者的负面影响，即使霸凌者可能认为他/她的实际行动并不比传统形式的欺凌行为更恶劣。
- 随着越来越多的人被引诱而成为霸凌行为的同谋者，控制电子传播的信息是很困难的。通过转发羞辱性的图片或信息，旁观者就成为霸凌行为的同谋者。

- 在网络霸凌中，霸凌者和霸凌目标的情况可能不同于其他形式的霸凌，因为网络霸凌可能发生于同辈之间，也可能发生于不同辈分之间。教师可能成为受害者，年龄和体型大小并不重要。
- 许多网络霸凌事件本身可以作为证据，因此受害者应保存信息，这一点是十分重要的。

## 网络霸凌和法律

**霸凌绝对不可接受的行为，学校充分认识到其有责任保护所有学校成员并为每个人提供安全而健康的环境。**

### 教育法

*圣约翰学院学校南京美之国幼儿园同时受中国当地法律的约束，英方相关法律法规在其运营过程中将作为参考和补充。*

- 《2006年教育与督导法案》（EIA 2006）列出了一些与网络霸凌更直接相关的法律权力。校长有权“在合理范围内”规制学生校外的行为。
- 该法案还为工作人员没收学生手机等物品提供了依据。

### 民法和刑法

- 没有一项特定法律规定网络霸凌是非法行为，但根据《防止骚扰法》（1997年）、《恶意传播法》（1988年）、《通信法》（2003年）、《淫秽出版物法》（1959年）以及《计算机滥用法》（1990年）等若干不同法案可以认定网络霸凌是一种刑事犯罪。

### 预防网络霸凌

与所有形式的霸凌一样，处理网络霸凌的最佳方式是在一开始就防止其发生。网络霸凌问题不存在单一的解决办法，但学校应至少采取以下措施以实施全面而有效的预防战略：

### 角色和职责

**园长同时担任指定的安全措施主管**，将全面负责协调和实施网络霸凌的预防和应对战略。园长应：

- 确保立即处理学校内外的所有网络霸凌事件，并根据学校的《反霸凌政策》、《行为政策》以及《安全措施和儿童保护政策》所规定的程序解决和/或向上级通报该事件。
- 确保定期审查和更新所有与安全措施（包括网络霸凌）相关的政策
- 确保所有工作人员均知悉他们需要向指定的安全措施主管报告有关网络霸凌的任何问题。
- 确保家长/照管人了解情况并每年关注网络霸凌政策，以便他们充分了解学校在保护学生及其福利方面的责任。可随时在学校网站上获取网络霸凌政策。

- 确保在每个学期开始时，将网络霸凌事务作为“保持安全项目”的一部分予以重新审查，并确保学生知悉报告霸凌事件的方式。（向他们感到安全的交际圈中的某个人
- 就工作人员在学校内外运用技术提供相关的明确指南，确保所有员工均了解自己的责任。所有工作人员都应签名，表示已阅读并理解《员工行为准则》。

### **计算机主管应当**

- 确保为学生在校内校外安全和健康地使用技术提供明确指导，包括如何管理他们的个人数据以及如何报告网上的侮辱和霸凌行为
- 每年在网络安全和技术的健康使用方面为家长/照管人提供培训
- 确保每年审查学校的《许可使用政策》、《儿童使用数字设备时的员工指南》以及《儿童数字设备使用政策》
- 每年就上述政策和程序为工作人员提供培训
- 每年就网络安全为工作人员提供培训
- 筹备并提供计算机课中有关网络安全的课程，培养学生的适应力，以在网络上保护自己和他人。
- 筹备课程并支持特殊需求生项目（PSE）的工作人员提供网络安全的课程，该课程旨在培养学生的适应力，以在网络上保护自己和他人。

### **信息技术支持和发展经理应当：**

- 确保存在足够的安全措施以过滤和监控不当内容，并就安全措施问题向指定的安全措施主管作出警示。学校使用第三方网络代理来过滤所有的互联网访问内容。互联网过滤器记录被拦截的站点，使信息技术支持能够立即向指定的安全措施主管报告问题。
- 确保学校的访客获取有关在校使用技术的明确指导。这包括如何向指定的安全措施主管报告任何安全措施问题。访问者将获得高度限制的访客账户，使用该访客账户无法访问任何个人数据，并且任何滥用该系统的行为将导致该系统的访问权被撤销。

### **财务主管应当：**

- 确保学校根据法定要求管理个人数据。学校参考英国《数据保护法案》（1998年）所承担的义务。在处理个人信息时应予以慎重考虑，当个人隐私需要受到保护时应予以尊重。只有那些需要获取个人信息的人员才能访问个人信息。在处理、收集、披露、保留或处置与学生或工作人员有关的信息时，应适用《数据保护法案》的原则。

### **学校理事会应当：**

- 任命一名理事负责福利事务，该理事将与指定的安全措施主管合作，确保有效实施与安全措施有关的政策和实践，包括防止网络霸凌。

## 员工指南

《行为准则》中包含了与使用电子通信和存储图像相关的安全操作指南。学校将根据《行为准则》处理不当使用技术的问题，这可能导致纪律处分。

如果您怀疑或被告知发生了网络霸凌事件，请遵循下面列出的行动方案：

### 手机

- 让学生将手机拿给您查看
- 清楚查看屏幕上与不当短信或图像有关的所有内容，包括日期、时间和姓名
- 制作口头信息的文字记录，并记录日期、时间和姓名
- 告诉学生保存该信息/图像
- 立即通知园长和负责安全措施主管，并将您了解到的信息传达给他们

### 电脑

- 让学生在屏幕上展示相关内容
- 让学生保存该内容
- 立即打印该冒犯性的内容
- 确保按正确的顺序排列所有页面，并且没有遗漏任何内容
- 通知高级管理层的人员并将您了解到的信息传达给他们
- 如果出现儿童保护问题，将遵循常规程序与儿童面谈并记录陈述内容。

### 在校内使用技术

**要求学校社群的所有成员都对健康使用技术承担起责任。**

除进行培训之外，还设置了以下程序：

- 要求所有工作人员签字确认其已阅读并理解《许可使用政策》。
- 要求所有工作人员签字确认其已阅读并理解《员工行为准则》。
- 要求所有工作人员签字确认其已阅读并理解《儿童使用数字设备时的员工指南》。

- 要求所有儿童均学习并理解《儿童数字设备使用政策》。

## 针对家长/照管人的指南

至关重要的是，家长/照管人和学校要共同努力，确保所有学生都意识到参与到可能被视为网络霸凌的任何行为中所带来的严重后果。家长/照顾者必须发挥自己的作用，并负责监督儿童的上网活动。

- 家长/照管人可以帮助确保他们的孩子了解学校的政策，其中最重要的是学校会如何严肃处理网络霸凌事件。
- 家长/照顾者还应向孩子解释与网络霸凌相关的法律问题。
- 如果家长/照管人认为他们的孩子是网络霸凌的受害者，他们应将冒犯性的内容保存下来（如有需要，可以将冒犯性的文字保存在他们的电脑或孩子的手机中），并确保在删除任何内容前已保存所有相关信息。
- 家长应尽快联系学校。
- 如果事件发生在假期，学校有权在学期之内和学期之外对校外发生的霸凌行为采取行动。
- 家长/照管人应参加学校计算机主管提供的有关网络安全的年度培训。

学校应确保家长/照管人了解儿童的网络霸凌政策和网络霸凌宣传单，以及网络霸凌政策中所规定的所有形式霸凌行为（包括网络霸凌）的处理程序。

### 家庭网络安全

有若干网站为家长/照管人提供了有用的建议，特别是关于对儿童在家中使用电脑进行监控的最佳方式。家长/照管人可尝试访问以下网站：

<http://www.thinkyou.know.co.uk/parents>

[www.saferinternet.org.uk](http://www.saferinternet.org.uk)

[Vodafoneigitalparenting.co.uk](http://Vodafoneigitalparenting.co.uk)

[www.childnet.com](http://www.childnet.com)

[www.anti-bullyingalliance.org.uk](http://www.anti-bullyingalliance.org.uk)

[www.nspcc.org.uk](http://www.nspcc.org.uk)

[www.cyberangels.org](http://www.cyberangels.org)

[Digizen](#)

我们的网站提供了以下有用的刊物：

[英国教育部针对网络霸凌为家长提供的建议](#)

[Childnet 网络霸凌宣传册](#)

[英国教育部：网络激进化中对社交媒体的使用](#)

指定的安全措施主管和行为主管是 Alice Wu 女士。