



编码: IIBGA-AR
修订/审查: 3/06/08;6/21/12;6/11/15;6/24/21
原始代码: SP IIBGA

学区电子通信系统使用指南**

定义

- 一. 根据《儿童互联网保护法》（CIPA）的定义，“技术保护措施”是指阻止或过滤互联网访问以下视觉描述的特定技术：
 - a. 淫秽，该术语在《美国法典》第 18 卷第 1460 节中定义；
 - b. 儿童色情制品，该术语在《美国法典》第 18 卷第 2256 节中定义；或
 - c. 对未成年人有害。
- 二. 根据 CIPA 的定义，“对未成年人有害”是指任何图片，图像，图形图像文件或其他视觉描述：
 - a. 从整体上看，就未成年人而言，诉诸对裸体、性或排泄的猥亵兴趣；
 - b. 以明显冒犯的方式描绘、描述或代表适合未成年人的内容，实际或模拟的性行为或性接触，实际或模拟的正常或性行为，或生殖器的猥亵展示；和
 - c. 总的来说，对未成年人缺乏严肃的文学、艺术、政治或科学价值。
- 三. CIPA 定义的“性行为 and 性接触”具有美国法典第 18 篇第 2246 节中赋予此类术语的含义。
- 四. 根据 CIPA 的定义，“未成年人”是指未满 17 岁的人。
 - a. 就董事会政策和本行政法规而言，未成年人将包括所有在地区学校就读的学生。
- 五. 学区定义的“不适当事项”是指与一般公共教育目的不一致的材料；以及学区的愿景、使命和目标，由学区决定。
- 六. “学区专有信息”由学区定义为学区工作人员为学区的商业或教育目的创建、制作或收集的任何信息，包括但不限于学生信息、员工信息、家长或赞助人信息、课程、表格和用于开展学区业务的类似项目。
- 七. “学区软件”由学区定义为使用学区资源获得的任何商业或员工开发的软件。
- 八. 「学区系统」或「电子通讯系统」包括所有学区电脑、设备、电邮、Google Apps、内联网及互联网接入。

学区基本责任

该学区将：

- 一. 根据需要指定工作人员，以确保协调和维护学区的电子通信系统，包括所有学区的计算机、设备、电子邮件和互联网接入；
- 二. 为员工提供适当使用学区电子通信系统的培训，包括学区政策和行政法规的副本。工作人员将向所有授权的系统用户提供类似的培训；
- 三. 禁止教职员使用个人电子设备下载学生、家长和教职员的个人身份信息，以及采购和采购信息。允许员工在符合区议会政策和行政法规的情况下使用个人电子设备访问学区的电子通信系统（请参阅员工用户协议）；
- 四. 在与滥用学区电子通信系统有关的任何调查中与地方、州或联邦官员充分合作；
- 五. 仅使用学区购买或批准学区使用的适当许可的软件、音频或视频媒体。学区将遵守有关使用、复制和分发受版权保护作品的法律要求以及适用的使用规定或许可协议；
- 六. 根据需要安装和使用病毒检测和删除软件；
- 七. 提供技术保护措施，防止成人和未成年人访问淫秽、儿童色情或未成年人使用计算机、对未成年人有害的视觉描述。主管或者委托人授权的其他个人可以禁用技术保护措施，以便为善意研究或其他合法目的酌情进行访问；
- 八. 禁止未成年人访问互联网上的不当内容；
- 九. 提供工作人员监督，以监控学生的在线活动，以防止未经授权的访问，包括“黑客”和其他非法在线活动，并确保未成年人在被授权使用电子邮件、社交媒体、聊天室、应用程序和其他形式的直接电子通信时的安全；
- 十. 为学生提供有关适当在线行为的教育，包括网络欺凌意识和反应，以及如何在社交网络和社交媒体网站、应用程序和聊天室中与其他个人互动；
- 十一. 确定哪些用户和站点（作为学区电子通信系统的一部分可访问）最适合学区的课程需求，并可能相应地限制用户访问；
- 十二. 确定哪些用户将有权访问该地区的电子通信系统；
- 十三. 通知相应的系统用户：
 - a. 学区始终保留对其计算机、设备、硬件、软件和数据的所有权和控制权。学区信息系统中传输、接收或包含的所有通信和存储信息均为学区的财产，仅用于授权目的。严禁将学区设备或软件用于未经授权的目的。为了保持系统完整性，监控网络礼仪并确保授权使用学区系统的人员遵守董事会政策，行政法规和法律，学校管理人员可以定期审查用户文件和通信；

- b. 在地区服务器上发送或接收、生成或存储的文件和其他信息（包括电子邮件）不是私有的，可能会受到监控。通过使用学区的系统，个人同意由授权的学区人员监督该使用。学区保留酌情访问和披露学区计算机、设备和学区拥有的电子邮件系统中包含的所有信息和数据的权利；
- c. 学区可以制定删除电子邮件的保留时间表；
- d. 董事会成员或雇员发送或接收的与公共事务交易有关的电子邮件可能是公共记录，并受州档案管理员保留和销毁规则的约束；
- e. 如果提出公共记录请求或对学区提起诉讼，则在学区的计算机、设备和电子邮件系统上输入或存储的信息和数据可能会被披露。从学区计算机、设备或电子邮件系统中“删除”或“清除”的数据可能会在学区认为必要时检索，用于以后的公共记录披露或纪律处分目的；
- f. 学区可以设置系统磁盘使用配额。学区可以允许系统用户通过向单位管理员或指定人员提交书面请求来增加配额，说明需要增加配额；
- g. 区电子通讯系统使用的密码将按区既定时间表更改；
- h. 不允许传输与 ORS 260.432 禁止的活动有关的任何通信或材料。

十四. 确保所有学生、教职员工和 非学校系统用户完成并签署协议，遵守学区电子通信系统政策和行政法规。所有此类协议将由学区以电子方式维护；

十五. 通知用户已知的版权侵权活动，并拒绝访问或删除材料。

电子通信系统接入

一. 访问学区电子通信系统的权限是:

经家长批准或在工作人员的直接监督下, 以及经技术总监或学区行政人员授权的地区志愿者、学区承包商或其他公众成员, 符合学区关于使用学区设备和材料的政策。

二. 在符合董事会政策和行政法规的情况下, 学生可能被允许使用学区的电子通信系统进行学校 and 教学相关活动。在符合董事会政策和行政法规的情况下, 允许个人使用学区拥有的计算机或设备, 包括互联网和电子邮件访问。

工作人员和董事会成员可能被允许使用学区的电子通信系统开展与学区的管理或教学需求相关的业务, 或在遵守董事会政策和行政法规的情况下进行与教育相关的研究。在符合俄勒冈州道德法、董事会政策和行政法规的情况下, 可能允许学区工作人员个人使用学区的系统或学区拥有的计算机或设备, 包括互联网和电子邮件访问。

工作人员和董事会成员可以使用学区的电子通信系统、学区拥有的计算机或设备(包括互联网和电子邮件访问)供个人使用, 其条款和条件与学区关于学区设备和材料使用的政策向公众提供的访问相同。

志愿者、地区承包商和其他公众人士在符合董事会政策、一般用途禁令和指南/礼仪以及本行政法规的其他适用规定的情况下, 可获准将学区的电子通讯系统用于个人用途。

一般使用禁令和指南/礼仪

学区电子通信系统的运作有赖于系统使用者的适当行为和适当使用。学生、教职员和其他被授予系统访问权限的人有责任遵守以下禁令和准则, 这些禁令和准则要求合法、道德和有效地使用学区的系统。

一. 一般使用禁令

严禁以下行为:

a. 尝试将学区的电子通信系统用于:

(1)未经授权募集资金;

(2)分发连锁信;

(3)未经授权销售或购买商品和服务;

(4)利用网络为任何商业或非法活动谋取经济利益;

(5)收集签名;

(6)会员驱动;

(7)传播有关政治运动的任何材料。

b. 试图在学区的系统上上传、下载、使用、复制或分发信息、数据、软件或文件共享音乐、视频或其他材料, 违反版权法或适用的使用规定或许可协议;

c. 试图降级、破坏、传播计算机病毒或破坏学区的设备、软件、材料或数据, 或学区系统的任何其他用户或连接到学区系统的任何机构或其他网络的设备、软件、材料或数据;

d. 未经校长明确同意, 试图将教师或学生的个人网站连接到学校或学区网站。任何有问题

的问题都应提交给技术总监。

- e. 试图发送、故意访问或下载任何文本文件或图片，或参与任何通信，包括但不限于可能被解释为：
 - (1) 对未成年人有害；
 - (2) 法律规定的淫秽或儿童色情内容或学区确定的不雅、粗俗、亵渎或猥亵内容；
 - (3) 法律不允许未成年人使用的产品或服务；
 - (4) 骚扰、恐吓、欺凌、威胁、威胁或偏见事件；
 - (5) 构成侮辱或战斗性言语，其表达本身就伤害或骚扰他人，包括仇恨和/或煽动暴力的象征；
 - (6) 由于其内容或分发方式而可能对学校或学校活动的正常有序运作造成重大或实质性干扰的可能性；
 - (7) 诽谤、诽谤、鲁莽或恶意虚假、可能引起民事责任、构成或促进歧视、刑事犯罪或以其他方式违反任何法律、规则、法规、董事会政策和/或行政法规。
- f. 试图通过学区系统未经授权访问任何涉及费用的服务，或试图在未经特别批准的情况下产生其他类型的费用。访问此类服务的用户将负责这些费用；
- g. 尝试发布或发布个人学生联系信息，除非获得单位管理员或指定人员的授权，并且符合与学生目录信息和个人身份信息相关的适用董事会政策。个人学生联系信息可能包括照片、年龄、家庭、学校、工作或电子邮件地址或电话号码，或其他未经授权的披露、使用和传播有关学生的个人信息；
- h. 试图在学区的电子通信系统上安排学生与任何人的会议，除非得到单位管理员或指定人员的授权，或者与学校或教育相关活动一致，并在必要时事先获得家长的批准；
- i. 试图通过在外部交流论坛中使用学区名称来代表学区代表自己例如，未经学区事先授权的社交媒体、聊天室；
- j. 尝试使用他人的帐户名或密码，未能向学区提供个人密码或访问用户未被授予访问权限的受限信息、资源或网络。
- k. 尝试加密区域计算机、设备或网络的密码。所有学区计算机、设备和服务器必须可供指定的学区技术人员完全访问；
- l. 未经授权在任何网站上使用该学区的名称、口号或徽标。

学生安全指南

- 一. 当学生的作品在互联网上发表时，不应识别其个人身份。在文本和视频示例中，仅当需要任何身份证明时才使用学生的名字和年级。
- 二. 学生的照片和视频应在不直接识别任何个别学生的情况下使用。
- 三. 学校不会在互联网上发布学校网站的平面图。
- 四. 学生将被指示不要回复并立即向他们的老师（或其他学校员工）透露他们收到的任何他们认为不合适或让他们感到不舒服的消息或图像。

投诉

学区在董事会政策 KL - 公众投诉和随附的行政法规中建立的投诉程序可用于处理有关违反政策和行政法规的投诉或疑虑。

违规/后果

一. 学生

- 一. 违反一般系统用户禁令的学生将受到纪律处分，包括开除和/或撤销对学区电子通信系统的访问权限，直至并包括永久丧失特权。
- 二. 违法行为可能会被举报给执法人员，并可能导致刑事或民事制裁。
- 三. 家长、学生和/或代表可以根据既定的地区程序对纪律处分提出上诉。

二. 员工

- 一. 违反一般电子通信系统用户禁令的员工应根据董事会政策、集体谈判协议和适用法律规定受到纪律处分，包括解雇。
- 二. 违法行为可能会被举报给执法人员，并可能导致刑事或民事制裁。
- 三. 违反适用的教师标准和实践委员会（TSPC）、俄勒冈州教育工作者胜任和道德绩效标准的行为将根据俄勒冈州行政规则 OAR 584-020-0041 的规定向 TSPC 报告。
- 四. 违反 ORS 244.040 的行为可能会报告给俄勒冈州政府道德委员会（OGEC）。

三. 其他

- 一. 其他违反一般电子通信系统用户禁令的访客用户将被暂停系统访问，直至并包括永久撤销权限。
- 二. 违法行为可酌情向执法官员或其他机构报告，并可能导致刑事或民事制裁。

电话/会员/其他费用

- 一. 对于因家庭使用学区电子通信系统而产生的任何会员资格、电话或互联网服务和/或相关费用，学区不承担任何责任或义务。
- 二. 因电话服务或为学区电子通信系统的家庭用户提供的互联网提供商服务而导致的任何争议或问题严格限于系统用户与其互联网服务提供商和/或电话服务提供商之间。

信息内容/第三方提供的信息

- 一. 尽管使用了学生保护措施，但建议系统用户和学生系统用户的家长，使用学区的电子通信系统可能会无意中提供可能被认为令人反感且与学区的愿景、使命和目标不一致的材料。家长应了解此类材料的存在，并相应地监控学生在家中使用学区电子通信系统的情况。
- 二. 系统用户、信息提供者、服务提供商或其他第三方个人表达的意见、建议、服务和所有其他信息是提供商的意见、建议、服务和所有其他信息，而不是学区的意见、建议、服务和所有其他信息。
- 三. 电子通信系统的用户可以在技术总监批准的情况下，从其他供应商处订购可通过学区电子通信系统访问的服务或商品。这些供应商不隶属于该地区。与订购的商品和服务有关的所有事项，包括但不限于购买条款、付款条件、保证、保证和交付，仅在供应商和电子通信系统用户之间发生。学区对供应商提供的任何商品或服务不作任何保证或陈述。地区工作人员和行政部门不得成为任何此类交易的一方，也不对因供应商的作为或不作为直接或间接引起的任何费用或损害负责。
- 四. 学区不保证电子通信系统执行的功能或服务，也不保证电子通信系统包含的信息或软件将满足系统用户的要求，也不保证电子通信系统不会中断或没有错误，也不保证缺陷将得到纠正。该地区的电子通信系统是按“原样，可用”的基础提供的。学区不作任何明示或暗示的保证，包括但不限于对电子通信系统提供的任何服务以及其中包含的任何信息或软件的适销性和特定用途的适用性。

** 在本政策中，父母一词包括法定监护人或父母关系中的人。法定监护人的地位和职责在 ORS 125.005（4）和 125.300 - 125.325 中定义。为了确定居住权的目的，确定个人是否在父母关系中行事，取决于对 ORS 419B.373 中所列因素的评估。其他目的确定取决于对这些因素的评估和根据 ORS 109.056 签署的授权书。对于特殊教育学生，父母还包括代孕父母、权利已转移的成年学生和 OAR 581-015-2000 中定义的养父母。