This *Student and Staff Technology and Network Acceptable Use Policy* rescinds and supersedes all previous policy, memoranda, and/or guidance promulgated by DCPS on this subject matter.

Chancellor Approval:

Effective: August 26, 2024

DISTRICT OF COLUMBIA PUBLIC SCHOOLS

学生和员工规范
使用技术和网络政策

I. 目的和范围

华府公立学校(DCPS)为学生和员工提供访问互联网、数据和网络系统(DCPS 网络)的权限。DCPS 还为学生和员工提供了使用计算机、平板电脑、设备和其他技术，例如打印机(DCPS 设备或技术)的权限。DCPS 向员工提供 DCPS 网络和 DCPS 技术以达到计划、教学和管理的目的；并提供给学生以用于教育、研究和职业发展。这项政策旨在：

- 建立规范使用 DCPS 网络和 DCPS 技术的标准；
- 围绕尽责使用人工智能设定期望；
- 防止未经授权和非法使用 DCPS 网络和 DCPS 技术；以及
- 为了遵守 2000 年《儿童互联网保护法》(CIPA)、《儿童在线隐私保护法》(COPPA)、《保护学生数字隐私法》以及所有其他适用的法律、规定、政策和程序。

本政策适用于所有 DCPS 学生、教职工、访客和其他使用 DCPS 网络或设备的人，并废除之前的 DCPS 学生和教职工规范使用技术和网络政策政策 (2021)。

II. 权威和适用法律[1]

资料来源	**引用的法规**
联邦法律	- 《儿童互联网保护法》(CIPA)，编为 47 U.S.C. § 254(h)(5) - 1998年《儿童在线隐私保护法》(COPPA)，编为 15 U.S.C. § 6501 *等系列条文*。 - 《社区儿童互联网保护法》，编为 47 U.S.C. § 254(l)
联邦法规	- 《儿童在线隐私保护规则》，16 CFR 312部分
华府法律	- 2016年《保护学生数字隐私法案》，D.C. Law 21-218，编为 D.C. Official Code 38-831.01 *等系列条文*。
华府市政规章(DCMR)	- 5-B DCMR § 2500 *等系列条文* – 学生纪律处分 - 6-B DCMR § 1610 – 员工渐进式纪律处分

[1] 本政策中的任何内容均不得取代联邦、州或地方法律。

III. 关键词及定义

人工智能(AI)是计算机科学的一个分支，研究计算机中智能行为的模拟。

DCPS 网络是指 DCPS 向所有 DCPS 学生和员工提供的互联网、数据和网络系统。

DCPS 员工是指可以使用 DCPS 网络和 DCPS 技术的所有 DCPS 教职工（全职或兼职）、合同工、代理、代表或志愿者、或代表 DCPS 行动的任何其他个人。

DCPS 技术是指 DCPS 向 DCPS 学生和员工提供的计算机、平板电脑、设备和其他技术。

开除是指根据当地教育机构的政策，因纪律原因将学生从其就读学校开除，持续时间为学年剩余时间或更长时间。

个人信息是指单独使用或与其他相关数据结合使用时可以识别个人身份的信息。个人信息包括但不限于姓名、家庭或实际居住地址、充当在线联系信息的网上姓名或用户名、以及包含个人图像或语音的照片、音频或视频文件。

渐进式纪律处分是指员工纪律系统提供对员工绩效和/或行为问题的分级回应。DCPS 渐进式纪律处分步骤包括口头咨询、警告、谴责和不利行为。

停学是指作为纪律处分的后果，暂时让学生离开其日常上课的环境/安排。在此期间，学生在校方人员的监督下留在校内，或必须离校。

IV. 要求

A. 一般

DCPS 向员工和学生提供并授权使用 DCPS 网络和 DCPS 技术。通过提供和授权使用技术资源，DCPS 不会放弃对 DCPS 提供的系统上的技术和材料的所有权或控制权。除下述内容外，通过 DCPS 网络或 DCPS 系统储存或传送的信息没有隐私，而且 DCPS 保留访问、查看、复制、储存或删除在 DCPS 技术或 DCPS 网络账户中储存的任何文件、和使用 DCPS 网络进行的所有沟通的权利。DCPS 对待储存在 DCPS 计算机上或使用 DCPS 系统传送的电子消息和文件如同对待任何其他学校财产一样。DCPS 工作人员可以查看文件和消息以进行调查、遵守法律要求、维护系统完整性，并在必要时确保技术和网络用户尽责行事并遵守本政策。DCPS 为学生或员工创建的所有帐户都可以受到 DCPS 的监控。

1. 学生

DCPS 将通过年度注册流程提供本政策的通知，并要求所有家长和成年学生确认收到此通知。学生和家长可能需要签署《学生技术和网络尽责使用协议》（《学生尽责使用协议》），该协议包含在附录中并可在 DCPS 网站上获取。《学生尽责使用协议》概述了使用 DCPS 技术或访问 DCPS 网络的学生的尽责使用和禁止的活动。学校还可能要求学生和家长签署所在学校的协议，这类协议详细说明了领取/退还技术设备的手续，列出了承担具体技术职责的学校职工并制定了学校的具体规则。

DCPS 每年为学生提供有关数字公民和在线安全的课程。学生必须完成数字公民和素养学生中心的课程，[2] 包括设备使用和维护单元，并且可能需要完成课程才能获得 DCPS 设备或帐户。

如果学生违反了这些规定， 将按照 DCPS 纪律条例和政策（包括安全和积极学生政策）[3]处理这类行为，并可能导致学生在较长的时间内无法访问 DCPS 网络或 DCPS 技术，只要学生可以通过其他方式参与并完成课堂学习，并且能够接受所有必要的特殊教育和英语学生服务。在某些情况下，不当行为也可以构成刑事犯罪。

2. 员工

DCPS 将通过入职流程向新员工提供本政策的通知，附录中包含的员工技术尽责使用协议（员工尽责使用协议）将在 DCPS 网站上提供，作为额外的持续参考。已分配 DCPS 设备的员工也可能会被要求在收到设备之前或收到设备时签署或重新签署员工技术尽责使用协议确认表。

华府政府、华府首席技术官办公室(OCTO)和/或 DCPS 可能要求员工完成与网络安全或相关主题有关的员工培训。未能及时完成这些培训或未能遵守本政策的员工可能会受到渐进式纪律处分。

B. 网络、电子邮件和应用程序

1. 网络

DCPS 向员工提供 DCPS 网络和 DCPS 技术以达到计划、教学和管理的目的；并提供给学生以用于教育、研究和职业发展。DCPS 网络允许员工和学生对 DCPS 信息和资源的内部访问、对 DCPS 批准的应用程序的使用以及对互联网的外部访问。DCPS 向学生提供 DCPS 网络（包括互联网）的访问，只是为了支持学生教育、研究和职业发展。使用 DCPS 网络是一种特权。违反本政策或相关政策任何部分的员工和学生可能会被取消其使用 DCPS 网络的特权，并可能受到纪律处分。

[2] *请参阅* https://dcps.instructure.com/enroll/Y8Y7KY。
[3] *请参阅* https://dcps.dc.gov/page/dcps-policies。

DCPS 为学校提供宽带上网，以便学校提供学术和运营服务。DCPS 保留优先安排宽带上网并限制某些对学术和运营服务造成负面影响的网络活动的权利。禁止网络用户使用 DCPS 网络访问被视为不当或非法的内容，其中包括但不限于色情的、淫秽的、非法的或煽动暴力的内容。

DCPS 不保证其提供的网络服务的功能或质量没有错误或缺陷。对于因使用网络或帐户而造成的任何索赔、损失、损害、花费或其他债务，DCPS 概不负责。个人因使用网络而产生的任何费用将完全由个人承担。DCPS 对通过使用系统获得的信息的准确性或质量概不负责，除非该信息是 DCPS 制作的内容任何非 DCPS 制作、可在网络或互联网上查阅的任何陈述应被视为作者的个人观点，而不是 DCPS、华府政府、其附属机构或雇员的观点。

2. 过滤器和监控

根据《儿童互联网保护法案》(CIPA)的规定，DCPS 必须保护学生免受在线威胁并对其进行教育，阻止其访问不当内容，并监视未成年人在学校网络上的互联网使用。[4]

DCPS 使用技术保护来拦截或筛除对淫秽的、色情的或对未成年人有害的图像/画面的互联网访问。除下文第 IV.G 节所述的内容以外，DCPS 保留监督和监控学生在线活动的权利，以及访问、查看、复制和储存或删除任何电子信息或文件以及必要时将其透露给他人的权利。学生在使用 DCPS 财产、DCPS 计算机网络或在网络中使用互联网、文件或电子邮件时，对保护自己的隐私应该没有任何期望，除非根据《保护学生数字隐私法案》的规定（请参阅下文第 IV.G 节）。

DCPS 还使用安全管理系统来分析和查看学生在线储存的文件内容、收发的 DCPS 电子邮件、DCPS 电子邮件附件以及网站链接中的内容。该系统拦截潜在的有害内容和图像，并在紧急情况下（例如对自己或他人的威胁或暴力）通知 DCPS 人员。

3. 应用

《儿童在线隐私保护法》(COPPA)要求面向 13 岁以下儿童的网站或在线服务的运营商、和实际上知道自己正在在线收集 13 岁以下儿童的个人信息的其他网站或在线服务的运营商在收集、使用或披露儿童的个人信息之前，征得可证实的家长的同意。[5]

[4] 47 U.S.C. 254(h)(5)(B).

[5] *请参阅* 16 CFR 312.5 部分。此要求也适用于家长先前同意的在收集、使用或披露信息方面的任何材料更改。运营商还必须为家长提供在不同意向第三方披露孩子的个人信息的情况下同意他们收集和使用孩子的个人信息的选项。

当 DCPS 与网站或在线服务商为收集个人信息签订合同以用于 DCPS 的使用和利益而不是其他商业目的时，运营商可以征得 DCPS 的同意，而无需直接获得家长的同意。[6]DCPS 将向家长提供同意通知书（DCPS 通过在 DCPS 网站上的所有遵守 COPPA 的网站的电子库存以及 DCPS 已经签约的和/或要求 13 岁以下的学生访问的在线服务来提供），其中包括指向每个运营商的隐私权政策的链接和家长如选择不同意须履行的手续。DCPS 的员工不得要求 13 岁以下的学生访问不遵守 COPPA 的网站和服务、或家长选择不让收集个人信息的任何遵守 COPPA 的网站和服务。

4. 访问控制

DCPS 实施安全访问控制措施，确保所有用户都可以适当地使用网络和技术，并锁定未经授权的访问和潜在的威胁。DCPS 根据年级和/学校或老师的要求，分配用户对 DCPS 网络、DCPS 电子邮件帐户、和 DCPS 授权的应用程序的访问，具体规定如下：

- **访问：**所有学生和员工必须使用其用户名和密码登录 DCPS 系统和设备。
- **电子邮件：**9 年级及以上的学生在成功地完成数字公民课程后将获得 DCPS 电子邮件帐户。其他年级的学生完成数字公民课程后， DCPS 员工可以酌情为其提供 DCPS 电子邮件帐户。患有特定残障的学生应该可以使用其 IEP 列出的测试和课堂调整来完成数字公民课程，这些调整可以包括大声朗读和重复指令、降低文本的阅读难度和简化内容以及其他调整。
- **应用程序：**DCPS 为所有 DCPS 员工和学生提供了对一组标准的获准使用的应用程序的访问。根据工作职责和当事人要求的一些应用程序为员工提供使用权限。学生可以使用获准的一套应用程序。根据学校和老师的要求，学生可以使用除了获准的一套应用程序之外的其他应用程序。
- **毕业或退学：**从 DCPS 毕业或退学的学生将无法再使用 DCPS 的技术或系统，包括应用程序和存储的材料。

5. 密码

所有 DCPS 发布的技术都需要密码保护，以防止未经 DCPS 授权的任何人使用，并且用户在登录学校计算机、网络和在线系统时必须遵守 DCPS 密码要求。作为定期更新密码过程的一部分，系统将自动提示用户满足这些 DCPS 的密码要求。

[6]有关遵守 COPPA 的更多信息，请参阅 https://www.ftc.gov/tipsadvice/business-center/guidance/complying-coppa-frequently-asked-questions。

学生和员工无权共享其密码或他们可能知道的任何其他 DCPS 学生或员工的密码，无论是出于无意还是违反本政策，并且必须格外小心，避免索要密码或其他个人信息的电子邮件诈骗。DCPS 要求学生参加数字公民和在线安全课程，学习如何避免这些诈骗以及安全使用技术的其他良好做法。

无法掌握数字公民课程的残疾学生无需遵守这些密码要求。

对密码的违规使用的处罚可能包括限制网络使用或取消帐户。此外，违规行为可能导致学生受到纪律处分和/或法律制裁（包括停学、开除和刑事起诉）。

6. 使用远程医疗

DCPS 允许员工和学生使用 DCPS 设备来参加远程医疗。虽然 DCPS 没有主动监视远程医疗的意图，但联邦法律要求学区扫描数据并监视学生在学校发放的设备上的活动，其中可能包括医疗记录或保存在设备硬盘驱动器上的其他文件。实时远程医疗将不会受到监视。如果机密数据储存在设备的硬盘驱动器上，它将在设备返回库存时被删除。

7. 视频会议

当 DCPS 员工和学生使用视频会议应用程序进行实时声音和视觉交流时，就会发生视频会议。教师和员工可以录制视频会议，并在以后提供给他们自己和学生。

员工不得在视频会议期间透露有关学生的个人身份信息。

员工和学生应向 DCPS 诚信办公室报告在视频会议期间可能发生的任何不当行为或相关行为。[7]员工和学生必须继续遵守 DCPS 员工权利和责任政策[8]、社交媒体政策[9]、以及有关员工-学生互动的任何其他适用政策、条例和法律。

8. 人工智能(AI)

与所有技术一样，学生和员工必须以负责任和道德的方式使用人工智能。学生和员工应使用人工智能工具作为学习的补充，而不是替代。DCPS 将通过数字公民和人工智能特定课程为学生提供有关人工智能的益处和风险的课程。

[7] 可以通过填写在线转介表联系诚信办公室，该表可在 https://dcps.dc.gov/page/office-integrity 上获取或发送电子邮件至 dcps.cio@k12.dc.gov。
[8] *请参阅* https://dcps.dc.gov/page/dcps-policies。
[9] *请参阅* https://dcps.dc.gov/page/dcps-policies。

尽管本政策的其他部分有所规定，但人工智能的以下用途是明确禁止的，并将受到额外审查：

- 欺凌和骚扰：禁止学生以可能伤害自己或他人的方式使用人工智能。禁止使用人工智能工具操纵媒体以冒充他人。
- 剽窃和作弊：禁止学生提交人工智能生成的作品作为其原创作品或使用人工智能回答测试、考试或其他作业问题（除非老师指示这样做）。

根据 DCPS 安全和积极的学校政策，[10] 工作人员必须实施纪律处分，从允许的纪律处分范围内最不严重的适当处分开始。这个范围可能会有所不同，从提供重新提交作业的机会到降低成绩。

a. 员工使用人工智能的其他注意事项

DCPS 维护着一份经过批准的人工智能增强工具列表，供学生学习，并将提供专业发展以支持这些工具的适当部署。如果教师和学校领导希望使用 DCPS 教育科技团队制定的列表之外的人工智能工具，该工具必须符合教育科技团队制定的标准，并且他们必须在购买和在课堂上或功课中使用之前提交人工智能工具批准表。这些标准和表格请参阅 EdTech SharePoint 网站：https://dck12.sharepoint.com/sites/DCPSEdTechInformationResources.

工作人员必须使用可信来源验证任何人工智能生成的内容的真实性，因为人工智能生成的内容可能包含错误或偏见。当使用人工智能进行沟通时，例如起草给家长的电子邮件时，工作人员有责任确保语言专业、准确和没有偏见。工作人员必须在使用前审查并批判性思考所有人工智能生成的内容。

C. 技术（包括计算机、笔记本电脑、平板电脑）

1. 设备支持

DCPS 为 DCPS 分发的技术设备提供基本的安装、并网和软件支持。设备必须定期连接到 DCPS 网络以接收软件更新和/或用于统计目的。所有 DCPS 分发的技术设备都需要密码保护，以防止丢失或被盗时未经授权的使用。

2. 损坏、丢失或被盗

员工是 DCPS 技术设备的管家，对由于疏忽而对财产造成的损坏、丢失或被盗可能会承担经济责任。疏忽的例子包括但不限于：

- 因把 DCPS 技术设备留在车辆或暴露于热、冷或潮湿的其他位置而造成的损坏；
- 由于洒泼的饮料或食物而造成的损坏；或
- 因把 DCPS 技术设备置于无人看管或不安全的位置而造成被盗。

[10] *请参阅* https://dcps.dc.gov/publication/safe-and-positive-schools-policy。

DCPS 工作人员只能使用 DCPS IT 团队分配给他们的设备，禁止拿走或使用分配给其他现任或过去员工的设备。

学生必须采取合理措施以防止设备损坏、丢失或被盗。如果学生设备损坏，学生所在学校的 DCPS 员工可以进行调查，以确定设备损坏是否因疏忽或蓄意破坏的行为而造成。该调查应考虑影响学生能否理解适当的设备护理的因素，包括年龄和任何相关的残疾。因*疏忽或蓄意破坏行为*而造成的损坏示例包括但不限于：

- 使用永久性马克笔在设备上涂鸦、使用尖锐物体蚀刻文字/图形或设备上的动物咬痕；
- 因设备处理不当或缺乏护理而造成多处损坏（例如，屏幕破裂、键盘损坏、按键丢失、或者笔记本电脑外壳多处有撞击痕迹或笔记本电脑/平板电脑收回时已经散架）；
- 强行损坏、使用尖锐或坚硬物品撞击造成的损坏、或物品卡入笔记本电脑 USB 或电源端口造成的损坏；
- 设备完全浸没在水或其他液体中；或
- 如果学生在一个学年内对三 (3) 件或更多设备造成损坏，则属于重复损坏模式。

对学生因疏忽或蓄意破坏行为而导致设备损坏的纪律处分，将根据 DCPS 安全和积极学校政策[11]、纪律处分条例和法律以及本规范使用政策确定。

学生不得因正常磨损或意外事故造成的损坏而受到处罚。*正常磨损*造成的设备损坏示例包括但不限于：

- 键盘上缺少按键；
- 因意外跌落导致屏幕破裂；
- 设备可能因意外掉落而造成的小部分（例如屏幕的角落/边缘）损坏；
- 意外地把液体泼溅到键盘上； 或
- 功率骤增造成的损坏。

如果 DCPS 技术丢失、被盗或损坏，学生必须通知老师或学校领导； 员工必须通知其主管和 DCPS 技术联系人。DCPS 将采取一切合理措施来找回丢失的设备，并确保设备中包含的任何信息的安全。DCPS 可以选择在设备上安装位置跟踪软件以定位被确认为丢失或被盗的设备，或远程禁用未应要求归还的设备。损坏的设备必须退还给 DCPS IT 团队(AssetAdmin@k12.dc.gov) 并且不得由学生、家长或工作人员处置。更换设备之前，必须首先由 DCPS IT 团队和 OCTO 进行评估。

[11] *请参阅* https://dcps.dc.gov/page/dcps-policies。

3. 学生夜间或在家使用设备

学校校长或 IEP 团队按照本政策的规定酌情做出决定： DCPS 学校员工可以为学生提供过夜或在家使用的 DCPS 设备。在分到供过夜或在家使用的设备之前，DCPS 学生和家长/监护人必须签署随附的《学生技术规范使用协议》。DCPS 学校员工必须遵守《学生数字隐私保护法案》提出的隐私要求，家长和学生应明白 DCPS 员工可以监控和使用这些设备。[12]

如果学生的 IEP 团队与 DCPS 辅助技术团队合作确定学生需要辅助技术设备以在家完成功课（例如，家庭作业、沟通），学生可以把这些设备带回家。学生在家里使用该技术时必须遵守 DCPS 的所有政策，就像在学校使用该技术时一样。有关辅助技术的更多信息，请访问 DCPS 辅助技术网站[13] 或联系 DCPS.AssistiveTech@k12.dc.gov 或学生的 IEP 团队。

D. 行为和规范使用

通过使用 DCPS 网络和 DCPS 技术，员工和学生同意遵守华府政府、 OCTO 以及 DCPS 发布的所有相关条例、政策和指南。员工和学生一旦发现有不当使用或违反协议的行为，应立即向教师、相关主管、管理人员或中心办公室的员工报告。[14]

员工和学生不得使用 DCPS 网络或 DCPS 技术（包括访问互联网、Intranet、协作工具、批量通信工具、社交媒体或电子邮件）以使用、记录、共享、上传、发布、邮寄、展示、储存或以任何其他方式传送以下内容、通信或信息：

1. 仇恨、骚扰、威胁、诋毁或诽谤；
2. 基于种族、肤色、宗教、国籍、性别、年龄、婚姻状况、个人相貌、性取向、性别认同或表达、家庭状况、家庭责任、入学、政治派别、遗传信息、残疾、收入来源、家庭内部犯罪的受害者身份、居住地或营业地点、或家庭暴力、性犯罪或纠缠行为的受害者身份或受害者的家庭成员身份的冒犯或歧视；
3. 根据任何适用法律（包括美国出口管制法或美国专利、商标或版权法）的规定，构成或加重任何刑事罪行，或引起民事责任；
4. 为了达到或支持任何淫秽或色情目的使用（包括但不限于传送、检索或观看）任何亵渎、淫秽或露骨色情内容的资料；
5. 为了达到煽动暴力、伤害他人或造成身体伤害、或骚扰、威胁或纠缠他人的目的索取或散布信息；
6. 包含病毒、特洛伊木马病毒、勒索软件或其他有害成分或恶意代码；
7. 构成垃圾邮件、网络诈骗、群发垃圾邮件或未经授权的广播电子邮件；

[12] *请参阅* D.C. Official Code § 38-831.03(a).
[13] *请参阅* https://dcps.dc.gov/page/assistive-technology%E2%80%AF。
[14]有关提交报告和投诉的更多信息，请参阅第五节。

8. 违反任何其他 DCPS 设备或网络的安全、或者构成对任何 DCPS 设备或网络的未经授权的访问、或企图规避任何安全措施；
9. 获得对另一个用户的 DCPS 网络帐户、文件或数据的访问权限、或向未经授权的第三方提供此类访问权限，或修改其文件、数据或密码；
10. 为达到欺骗的目的，冒充一名在世或已故的授权人士、组织、企业或其他实体；
11. 降低 DCPS 网络或技术的性能、造成安全风险、或以其他方式威胁其完整性或有效运行；
12. 剥夺授权用户对 DCPS 网络或技术的访问；
13. 获得对超出授权范围的 DCPS 技术或华府网络的访问；
14. 未经授权或非法进入 DCPS 网络系统；
15. 在未经授权或没有采取适当的安全措施的情况下泄露机密或专有信息，包括学生记录信息；
16. 在未经授权或没有采取适当的安全措施的情况下披露或传送可识别个人身份的学生信息、视频和照片；
17. 以违反华府法律、联邦法律、规定、政策或指南的方式共享有关学生或 DCPS 人员的保密信息；
18. 共享 DCPS 电子邮件地址或群发列表以达到违反此政策或任何其他 DCPS 政策的用途；
19. 促使或构成任何形式的下赌注或赌博；
20. 安装、下载或使用未经授权或没有执照的软件或第三方系统；
21. 在网上访问、散布、下载或使用未经授权的游戏、程序、文件、电子媒体和/或独立应用程序，从而可能会对 DCPS 网络造成威胁；
22. 以任何方式促进或参与未经授权的抽奖活动或筹款活动；
23. 以任何方式促进或参与党派政治活动；
24. 以任何方式促进或参与与代表员工的工会或其他组织有关的内部政治或选举活动；
25. 从事私人业务、商业或其他活动以谋取个人经济利益；
26. 散布有关其他用户的密码或安全系统的未经授权的信息；
27. 伪造、篡改或在未经授权的情况下更改、添加或删除 DCPS 网络或任何学校系统上的数据；
28. 访问或使用 DCPS 网络上的数据以达到个人使用的目的；
29. 促成或参与涉及到学生的但与学业或学校主办的课外活动无关的任何活动或关系，除非事先得到校长和学生的家长/监护人的书面授权；
30. 违反为特定技术、应用程序或 DCPS 网络系统明确规定的使用条款；
31. 构成会干扰学校或办公室正常有序运行的使用；
32. 侵入（故意通过非法手段或未经授权获得访问） DCPS 网络以访问未经授权的信息，或以其他方式规避信息安全系统；
33. 从事不当性行为，包括强迫性性接触、不雅暴露、传递性暗示图像或其他性活动；或
34. 违反本政策或任何其他 DCPS 政策阐明的任何禁止规定。

学生、员工和其他用户不得与任何其他个人共享其 DCPS 分发的设备或 DCPS 分发的网络登录信息。使用他人的 DCPS 分发的设备或 DCPS 分发的网络登录信息、允许未经授权的用户使用自己的 DCPS 分发的设备或 DCPS 分发的网络登录信息、或通过共享登录信息或任何其他方式促进对任何其他人的 DCPS 分发的设备 或 DCPS 分发的网络登录信息的未经授权的使用是严格禁止的。

E. 个人媒体技术

未经主管校长或其指定人员的明确书面授权，学生不得在 DCPS 网络上使用个人技术设备。DCPS 对学生个人电子设备的维护和安全概不负责，也不对此类设备的失窃承担任何责任。DCPS、OCTO 及其工作人员无需为寻求在学校或 DCPS 网络上使用个人电子设备或访问 DCPS 设备上的个人媒体帐户的学生提供技术支持，但对在这些个人设备上使用基于网络、经 DCPS 批准的应用程序的支持除外。除非如本节中下文所述，否则 DCPS 保留在学生使用个人设备来访问 DCPS 网络时在其设备上实施安全措施和在发现其个人设备的使用违反了 DCPS 政策时把它从 DCPS 网络中删除的权利。

F. 学生个人媒体帐户和技术设备的隐私

1. 学校特定的学生个人媒体帐户和技术政策

如果学校有与学生个人媒体帐户和技术设备相关的附加规则，校长必须以书面形式通知学生和家长。

2. 个人媒体帐户和学生技术设备的一般隐私

除非满足第 IV.G.3 节中所述的例外情况，否则 DCPS 不会对学生或准学生采取或威胁采取不利行动，其中包括纪律处分、开除、退学、拒绝录取或禁止参加课程或课外活动，因为这名学生或准学生拒绝：

- 披露用于访问学生的个人媒体帐户或个人技术设备的用户名、密码或帐户认证的其他方式；
- 在校方人员在场的情况下访问学生的个人媒体帐户或个人技术设备，以使校方人员可以查看该帐户或设备上的数据；
- 将个人添加到可以查看学生的个人媒体帐户或访问学生的个人技术设备的用户列表中；或
- 更改与学生的个人媒体帐户或个人技术设备相关的隐私设置。[15]

如果 DCPS 通过其他合法方式无意中收到了学生或准学生的个人媒体帐户或个人技术设备的用户名、密码或帐户认证的其他方式，DCPS 将：

[15] D.C. Official Code § 38-831.04(a).

- 不得使用该信息访问学生或准学生的个人媒体帐户或个人技术设备；
- 不与任何人共享该信息；并且
- 立即或尽快在合理可行的情况下删除该信息。[16]

本节中的任何内容均不能阻止 DCPS：

- 查看有关学生或准学生公开可用的信息；
- 要求学生或准学生自愿共享可从个人媒体帐户或个人技术设备上访问的特定内容以确保遵守适用法律或 DCPS 政策，前提是该要求符合本政策的规定；
- 禁止学生或准学生在上学期间或在学校期间访问或操作个人媒体帐户或个人技术设备；
- 监控 DCPS 网络的使用情况；或
- 废除学生对 DCPS 网络或 DCPS 技术的全部或部分使用。[17]

3. 个人媒体帐户和学生技术设备的隐私例外

在以下违反政策或生命或安全受到迫在眉睫的威胁的情况下，DCPS 员工可以搜查学生的个人媒体帐户或个人技术设备，或命令学生提供可从学生的个人媒体帐户或个人技术设备中获取的数据。

a. 违反政策

如果 DCPS 员工合理地怀疑学生对个人媒体账户或个人技术设备的曾经使用或当前使用进一步违反了 DCPS 政策，并且合理地怀疑个人媒体账户或个人技术设备含有涉嫌违规的证据，DCPS 员工可以搜查学生的个人媒体帐户或个人技术设备，或命令学生提供可从学生的个人媒体帐户或个人技术设备中获取的数据。[18]

在进行此类搜查或命令学生找出此类数据之前，DCPS 员工必须：

- 记录导致需要进行搜查或找出数据的合理的怀疑；并
- 把对学生涉嫌违规的怀疑以及要搜索的或者学生将奉命找出的数据或组成部分通知学生及其家长/监护人。[19]

只有当在扣押的预先通知时间不超过 48 小时、个人技术设备安全储存在 DCPS 物业中并且在扣押的预先通知期间无法访问时，DCPS 才能扣押学生的个人技术设备以防止学生在发出此要求的通知之前删除数据。[20]

[16] D.C. Official Code § 38-831.04(b).
[17] D.C. Official Code § 38-831.04(e).
[18] D.C. Official Code § 38-831.04(c)(1)(A).
[19] D.C. Official Code § 38-831.04(c)(1)(B).
[20] D.C. Official Code § 38-831.04(d).

搜查或命令交出必须限于可从帐户或设备或设备的组件中获取且可能会提供涉嫌违规证据的数据，而且任何人不得复制、共享或转移通过搜查或命令交出的但与引发搜查的涉嫌违规无关的数据。[21]

b. 对生命或安全的急迫威胁

DCPS 员工可以搜查学生的个人媒体帐户或个人技术设备，或命令学生找出可从学生的个人媒体帐户或个人技术设备中获取的数据，前提是员工必须这样做以应对对生命或安全的急迫威胁。[22]

任何搜查或命令交出的范围都必须限于此目的，而且 DCPS 必须在搜查或命令交出的72小时内，向学生及其家长提供关于引发搜查的确切威胁和获取的数据的书面说明。[23]

V. 政策实施要求

所有 DCPS 的学生和员工都必须遵守本政策阐明的规定。为了支持其实施，校长应每年让教职工了解要求的活动和时间表。该政策的实施将通过中央监督程序得到加强，该程序包括定期数据审查、记录采样、基础文档审查和现场视察（根据需要）。该程序将确保我们共同建立一个持续改进的体系并防止违规行为。如需相关问题、培训或实施的关键指导和支持，请访问dcps.dc.gov。

DCPS 致力于为每一位学生提供公平、卓越、透明和问责的服务。如果对这项政策有任何疑问或想要举报可能的违规行为，请填写在线转介表[24]或发送电子邮件至 dcps.cio@k12.dc.gov，与首席诚信官(CIO)联系。

[21] D.C. Official Code § 38-831.04(c)(1)(C)-(D).
[22] D.C. Official Code § 38-831.04(c)(2)(A).
[23] D.C. Official Code § 38-831.04(c)(2)(B)-(C).
[24] *请参阅* https://dcps.dc.gov/page/office-integrity。

附录

以下文件作为附录包含在内：

- 学生技术尽责使用协议；
- 学生技术尽责使用协议确认表；和
- 员工尽责使用技术协议确认表。

学生技术尽责使用协议

作为负责任的技术用户：

A. 我将尊重我的 DCPS 设备，小心不要把它掉落或损坏。

- ❑ 我将遵守有关借还 DCPS 设备的学校规定。
- ❑ 如果我的 DCPS 设备被损坏或无法正常工作，我将立即向老师或员工报告。
- ❑ 每当我不使用设备时，我都会将它放在室内安全的位置。

B. 我会保护我的个人信息。

- ❑ 我不会与任何人共享我的 DCPS 设备、用户名或密码，（除非我是幼教学生或需要支持才能使用我的帐户的学生）。
- ❑ 完成功课后，我将把功课保存在 DCPS Office365 OneDrive 中，并退出我的帐户和程序。
- ❑ 如果我认为或知道有人使用了我的帐户，我会立即通知老师。

C. 我只会将我的设备用于功课。

- ❑ 只有在老师允许的情况下，我才会下载、安装或使用软件、应用程序、浏览器扩展或媒体文件。
- ❑ 我会避免使用不适当、冒犯性或非法的资源。如果我在网上看到不适当的材料，我会立即向老师或工作人员报告。

D. 我将运用我的数字公民技能并善待他人。

- ❑ 我会使用尊重和适当的语言。
- ❑ 我会适当参考别人的作品，不会抄袭。
- ❑ 在网上分享信息之前，我会核实信息。
- ❑ 我将以负责任和有道德的方式使用人工智能，尊重所有人的隐私，不欺凌或骚扰他人，在功课上不抄袭或作弊。

不负责任的技术使用的后果

根据 DCPS 学生纪律条例和政策，你将在一段时间内无法访问 DCPS 网络或 DCPS 技术。在某些情况下，DCPS 员工可以随时搜索和查看位于 DCPS 网络上或保存在 DCPS 设备中的所有文件。在某些情况下，DCPS 员工可以获准搜查你的个人媒体帐户或设备，或要求你提供你的个人媒体帐户或设备中的数据。

被盗或意外被损坏的设备的规程

如果你的设备被盗或损坏，你必须立即通知教师或工作人员，因为 DCPS 必须在涉嫌盗窃后的五个日历日内向警方提交报告，以便追踪设备。你无需承担因设备被盗或意外损坏而产生的相关费用。在这种情况下，我们非常感谢你与 DCPS 的合作。

不可接受的技术使用示例：

- 在 DCPS 设备旁吃喝；
- 在 DCPS 设备上书写、绘画或粘贴贴纸；

- 下载、安装或运行任何类型的文件，包括音乐和视频文件、网站、软件、应用程序、浏览器扩展或媒体，除非教师允许；
- 使用应用程序或插件尝试更改安全设置或互联网内容过滤器；
- 将 USB 驱动器（即闪存驱动器）插入设备，除非得到老师的批准；
- 搜寻、保存、传播、或展示仇恨性、淫秽、庸俗资源等；
- 利用 DCPS 网络从事任何违法或犯罪行为；
- 访问在线游戏、社交媒体、消息应用程序或群聊，除非这些活动与学业相关并且有教师或工作人员监督该活动；
- 欺凌、骚扰、威胁或恐吓他人；
- 使用他人的登录名或密码；以及
- 未经他人许可，创建或发布他人的图片、音频或视频记录。

DISTRICT OF COLUMBIA
PUBLIC SCHOOLS

学生尽责使用技术协议
确认表

学生：我已阅读 DCPS 学生和员工技术和网络规范使用政策以及学生技术尽责使用协议，或者有人已阅读并向我解释。

家长/监护人：我已阅读并与我的孩子讨论了 DCPS 学生和员工技术和网络规范使用政策以及学生技术尽责使用协议。

1. 我同意根据协议和规范使用政策列出的规则尽责使用所有 DCPS 设备和 DCPS 网络。我知道：如果我不遵守这些规则，我可能会面临 DCPS 纪律处分规则和政策列出的后果，并且我使用 DCPS 设备和 DCPS 网络的能力可能会受到限制。

2. 我知道，如果我看到或以其他方式发现有人在使用 DCPS 设备或 DCPS 网络欺凌、恐吓、威胁、骚扰或伤害他人，我应当向老师或员工举报。我知道我的报告将被保密，并且 DCPS 不会容忍对我举报这类事件的任何报复。

3. 如果我获得了设备，我了解该设备仅根据 DCPS 学生和员工技术和网络规范使用政策借给我。DCPS 根据2016年《保护学生数字隐私法案》的规定收集数据并监控笔记本电脑的使用情况。

4. 如果我丢失或故意或不小心损坏了 DCPS 设备，我可能会面临 DCPS 的适当纪律处分。我将需要与 DCPS 开会，确定丢失或损坏的原因，并学习负责任的设备看护。

5. 如果我获得了设备，我了解必须根据要求将它退还给我的学校技术联系人或 DCPS IT 团队 (AssetAdmin@k12.dc.gov)。如果我没有按要求归还设备，设备可能会被远程禁用，并且可能会向我的家人收取费用。

6. 我了解，一旦我从 DCPS 毕业或取消注册，我将无法再使用 DCPS 技术或网络。

DISTRICT OF COLUMBIA
PUBLIC SCHOOLS

员工尽责使用技术协议
确认表

我已阅读《DCPS 学生和员工技术和网络规范使用政策》。

1. 我同意根据规范使用政策中列出的规则尽责使用 DCPS 网络和向我发放的任何 DCPS 设备。我知道：如果我不遵守这些规则，我可能会面临 DCPS 纪律处分规则和政策以及华府法律和法规列出的后果。

2. 如果 DCPS 向我发放笔记本电脑，我承认该笔记本电脑归 DCPS 所有。借给我的笔记本电脑仅用于学习目的，我按照《DCPS 学生和员工规范使用技术和网络政策》使用它。

3. 如果 DCPS 向我发放笔记本电脑，在我借用笔记本电脑期间， 对由于我的疏忽或故意行为而造成的损坏，我将负责承担与维修相关的任何费用。

4. 如果 DCPS 向我发放了笔记本电脑，在我离开学校系统或根据要求时，必须将笔记本电脑归还给 DCPS IT 团队(AssetAdmin@k12.dc.gov)。如果 DCPS 要求时我未能归还此设备，我可能会支付费用。