

DCPS学生和员工规范使用技术和网络政策

I. 目的

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向员工提供其网络和技术以达到计划、教学和管理的目的；并提供给学生用于教育、研究和职业发展。这份DCPS学生和员工安全和规范使用技术和网络政策的目的是：

- 1) 建立规范使用DCPS网络和DCPS技术的标准；
- 2) 防止未经授权和非法使用DCPS网络和DCPS技术；以及
- 3) 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学生和员工（统称用户），并废除了 [DCPS 学生 安全使用互联网和技术政策 \(2009\)](#)。

II. 权威

资料来源	引用的法规
联邦法（USC）	<ul style="list-style-type: none"> - 《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 - 《儿童互联网保护法》（CIPA），编为47 U.S.C. § 254(h)(5)
联邦法规（CFR）	<ul style="list-style-type: none"> - 《儿童在线隐私保护规则》，16 CFR 312部分
华府法规（华府法典）	<ul style="list-style-type: none"> - 2016年《保护学生数字隐私法案》（华府法规 21-218），编为《华府法典》38-831.01等系列条文。
华府市政规章（DCMR）	<ul style="list-style-type: none"> - 5-B华府市政规章 § 2500等系列条文（学生纪律处分） - 6-B华府市政规章 § 1610（员工分阶段纪律处分）

III. 关键词

DCPS员工：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网络：DCPS向其所有学生和员工提供的互联网、数据和网络系统。

DCPS技术：DCPS向其所有学生和员工提供的计算机、平板电脑、设备和其他技术。

个人信息：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、用作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。

停学：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。

开除：由于学生受到纪律处分，其注册的学校在学年剩余时间或更长时间将其除名。

循序渐进的纪律处分：员工纪律系统提供对员工绩效或行为问题的分级回应。DCPS循序渐进的纪律处分步骤包括口头咨询、谴责、纠正措施和不利行为。

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不会放弃对系统材料或系统文件中包含的材料控制。除下述内容外，通过DCPS网络或DCPS系统存储或传送的信息没有隐私，而且DCPS保留访问、查看、复制、存储或删除在其技术或网络账户中储存的任何文件、和使用其网络进行的所有通信的权利。对存储在DCPS计算机上或使用DCPS系统传送的电子消息和文件视如学校财产。DCPS员工可以查看文件和消息以维护系统完整性，并在必要时确保用户行为的负责性。DCPS员工可以监视由DCPS为学生创建的或应DCPS请求由学生创建的所有学生帐户。

B. 网络、电子邮件和应用程序

1. 网络

DCPS向员工提供其网络和技术以达到计划、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向学生提供网络（包括互联网）的使用，只是为了支持学生教育、研究和职业发展。使用DCPS网络是一种特权而不是一种权利。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。

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引发的任何索赔、损失、损害、花费或其他债务，DCPS不承担任何责任。个人因使用网络而产生的任何费用将完全由个人承担。除非从DCPS网站或华府政府网站获得信息，否则DCPS对通过使用系统获得的信息的准确性或质量概不负责。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要求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。¹

DCPS使用技术保护来阻止或筛除网上淫秽的、色情的或对未成年人有害的图像/画面。除下文第IV.G节所述的内容以外，DCPS保留监督和监视学生的在线活动、并访问、查看、复制和存储或删除任何电子信息或文件以及视需要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（请参阅下面的第IV.G节）。

DCPS还使用安全管理系统来分析和查看学生在线存储的文件内容、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，征得家长的同意。²

¹47 U.S.C. 254(h)(5)(B)。

²参阅 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重大变更。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收集和使用孩子的个人信息的选择。

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。DCPS将向家长提供同意通知书（DCPS通过所有遵守COPPA的网站上的自家网站以及已经签约的和/或要求13岁以下的学生访问的在线服务的电子库存来提供），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，以确保所有DCPS用户都可以适当地使用网络和技术，并锁定未经授权访问和潜在的威胁。DCPS会根据年级和学校或老师的要求，分配学生对DCPS网络、DCPS电子邮件帐户、和DCPS授权的应用程序的访问权，具体规定如下：

- **网络：**虽然为所有学生提供了各自的个人认证信息和密码，但从学前班到2年级的学生可以使用学校提供的通用登录名。3年级及以上的学生**必须**使用其个人认证信息和密码来登录。
- **电子邮件：**9年级及以上的学生成功完成数字公民课程后，将为其提供DCPS电子邮件帐户。
- **应用程序：**DCPS为其所有员工和学生提供了一组标准的获准使用的应用程序。根据员工的工作职责提供使用相关应用程序的权限。根据学校和老师的要求提供学生使用相关应用程序的权限。

5. 密码

登录学校计算机、网络和在线系统时，DCPS用户必须遵守DCPS密码的规定。用户无权共享其密码，并且必须格外小心，以避免申请密码或其他个人信息时的电子邮件骗局。

对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. 在线安全、数字公民和网络安全

DCPS将为学生提供有关数字公民和在线安全的年度课程。华府政府、华府首席技术官办公室和/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可能会导致循序渐进的纪律处分。

³有关遵守COPPA的更多信息，可从联邦贸易委员会获得：<https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>。

C. 技术（包括计算机、笔记本电脑、平板电脑）

1. 设备支持

DCPS为发行自己的电子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发行的电子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、丢失和被盗

员工是DCPS技术的管家，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技术设备留在暴露于热、冷或潮湿的车辆或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。

学生必须采取合理措施以防止设备损坏、丢失或被盗。将根据DCPS纪律规定和政策确定对造成损害的学生的纪律处分。任何违规使用设备的行为都可能导致学生长期失去使用DCPS设备的特权，只要他们可以通过其他方式参与并完成课堂学习，并且能够获得所有必要的特殊教育或英语学习生服务。

如果DCPS技术设备丢失、被盗或损坏，用户必须立即通知DCPS员工。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性。DCPS可能会选择在设备上安装位置跟踪软件，以查找被确认为丢失或被盗的设备。

3. 学生夜间或在家使用

未经主管校长或主管校长指定人员的明确书面授权，DCPS学校员工不得向学生提供DCPS设备以让学生在夜间或在家使用。如果此类做法获得授权，那么负责监督此类做法的DCPS员工必须确保遵守《学生数字隐私保护法》中的隐私规定。⁴

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、华府首席技术官办公室以及DCPS发布的所有相关法规、政策和指南。员工一旦发现有不当使用或违反协议的行为，应立即通知教师、适当的主管、领导或中心办公室的员工。⁵

用户不得使用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、显示、存储或以任何其他方式传送以下任何不可接受的内容、通信或信息：

⁴具体内容请参阅华府法典第 § 38-831.03(a)条。

⁵有关提交报告和投诉的更多信息，请参见第五节。

1. 仇恨、骚扰、威胁、诋毁或诽谤；
2. 对基于种族、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、性犯罪或缠扰行为的受害者或受害者的家庭成员的冒犯或歧视；
3. 根据任何适用法律（包括但不限于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）任何猥亵的、淫秽的或性暴露内容的资料；
5. 为了达到煽动暴力、伤害他人或造成身体伤害、或骚扰、威胁或缠扰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部分或恶意代码；
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；
8. 违反任何其他计算机或网络的安全、或者构成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、或修改其文件、数据或密码；
10. 冒充任何一名活着或死去的人、现有的或已不存在的组织、企业或其他实体；
11. 降低DCPS网络或技术的性能，引发安全风险或威胁其完整性或有效运行；
12. 剥夺授权用户访问DCPS网络或技术的权限；
13. 获得超出授权范围的DCPS技术或华府网络访问的权限；
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，以用于违反此政策或任何其他DCPS政策；
19. 促使或构成任何形式的下赌注或赌博；
20. 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/或独立的应用程序，从而可能会对DCPS网络造成威胁；
21. 以任何方式促进或参与未经授权的抽奖活动或筹款活动；
22. 以任何方式促进或参与党派政治活动；
23. 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；
24. 从事私人业务、商业或其他活动，以谋取个人经济利益；
25. 散布有关其他用户密码或安全系统的未授权信息；
26. 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；
27. 访问或使用DCPS网络上的数据供个人使用；
28. 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；
29. 安装、下载或使用未经授权或未经许可的软件或第三方系统；

-
30. 违反为特定技术、应用程序或DCPS网络系统指定的使用条款；
 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（包括不受欢迎的性接触、不雅的暴露、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政策中阐明的任何禁止规定。

E. 学生行为和负责任使用

所有学生和家长必须每年签署附录中的《学生技术和网络负责任使用协议》（也称为《学生负责任使用协议》）。《学生负责任使用协议》概述了使用DCPS技术或访问DCPS网络的学生负责任使用和禁止的活动。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。

如果学生违反了这些规定，DCPS将按照学生纪律法规和政策处理这类行为。这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，并且能够获得所有必要的特殊教育或英语学习生服务，在某些情况下，不当行为也可能会构成刑事犯罪。

F. 个人媒体电子设备

校长根据DCPS和华府首席技术官办公室（OCTO）的政策酌情允许学生使用个人电子设备。DCPS对学生个人电子设备的维护和安全不承担任何责任，也不对此类设备的失窃承担任何责任。DCPS员工无需为试图在学校或DCPS网络上使用获准的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。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。

G. 学生个人媒体帐户和电子设备的隐私

1. 各所学校发布的学生的个人电子设备和媒体帐户政策

校长必须把学校的学生个人电子设备和媒体帐户政策以书面形式通知学生和家长。校长可以随时以任何理由更改此类政策，但前提是必须在实施更改过的政策的至少前一天以书面形式通知学生和家长。

2. 个人媒体帐户和学生电子设备的一般隐私

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、拒绝录取或拒绝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、密码或其他帐户认证方式；
 - 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。⁶

如果DCPS或DCPS员工通过合法手段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、密码或其他帐户认证方式，那么DCPS和/或DCPS员工将：

- 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；
- 不与任何人共享信息；并且
- 立即或尽快在合理可行的范围内删除信息。⁷

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访问的特定内容，以确保遵守适用法律或DCPS政策，前提是该请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
- 废除学生全部或部分使用DCPS网络或DCPS技术的权限。⁸

3. 个人媒体帐户和学生电子设备的隐私例外

在以下两种情况下，DCPS员工可以搜索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帐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帐户或个人技术设备含有涉嫌违规的证据，那么DCPS员工可以搜索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该学生的个人媒体帐户或个人技术设备获取的数据。⁹

在进行此类搜索或命令学生找出此类数据之前，DCPS员工必须：

⁶ 华府法典第 § 38-831.04(a)条。

⁷ 华府法典第 § 38-831.04(b)条。

⁸ 华府法典第 § 38-831.04(e)条。

⁹ 华府法典第 § 38-831.04(c)(1)(A)条。

- 记录导致需要进行搜索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。¹⁰

只有当在扣押的预先通知时间不超过48小时、个人技术设备安全存储在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。¹¹

搜索或对学生下达的命令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、共享或转移通过搜索或强制获取的但与引发搜索的涉嫌违规无关的数据。¹²

b. 对生命或安全的急迫威胁

DCPS员工可能会搜索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获取的数据（如果员工必须这样做，以应对对生命或安全的急迫威胁）¹³

任何搜查或对学生下达的命令的范围都必须限于此目的，而且DCPS必须在搜查或对学生下达命令的72小时内，向学生及其家长提供关于引发搜索的确切威胁和获取的数据的书面说明。¹⁴

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，校长应每年让员工了解所需的活动和时间表。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访问（根据需要）。该框架将确保我们共同建立一个持续改进的系统并防止违规行为。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致力于为每个学生提供公平、卓越、透明和负责的服务。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 [在线转荐表](#) 与首席诚信官（CIO）联系并发送电子邮件至 dcps.cio@dc.gov。

VI. 附录

参见下一页：学生负责任地使用技术协议

¹⁰ 华府法典第 § 38-831.04(c)(1)(B)条。

¹¹ 华府法典第 § 38-831.04(d)条。

¹² 华府法典第 § 38-831.04(c)(1)(C)-(D)条。

¹³ 华府法典第 § 38-831.04(c)(2)(A)条。

¹⁴ 华府法典第 § 38-831.04(c)(2)(B)-(C)条。

2020-21学年学生负责任地使用技术协议

所有DCPS学生必须在老师和DCPS员工的指导下负责任地使用DCPS计算机、其他DCPS技术（“DCPS设备”）、和DCPS网络，具体规定如下：

我负责妥善保管DCPS设备。

- 我将以自豪和尊重的态度对待我的DCPS设备，小心不要把它掉落。
- 我将遵守有关借还DCPS设备的学校规定。
- 我不会在DCPS设备附近吃喝。
- 我不会在DCPS设备上涂写乱画、或张贴贴纸。
- 随身携带DCPS设备时，我将其关闭以保护其屏幕。
- 我不会倚靠在DCPS设备上或在它的顶部放置任何可能损坏屏幕的重物。
- 我不会损坏耳机、手写笔和键盘等配件。
- 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。

我对自己的DCPS账户负责。

- 我将不与他人共享自己的用户名和密码。
- 完成工作后，我将保存工作并退出所有帐户和程序。
- 我对通过我的帐户完成的所有活动负责。
- 如果我认为或知道有人使用了我的帐户，我会告诉老师。

我负责帮助保护DCPS网络的安全。

- 除非得到老师的许可，否则我不会下载、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）。
- 我不会下载或安装应用程序或浏览器插件来绕过互联网内容过滤器，尝试更改安全设置或互联网内容过滤器，或以任何方式干扰网络。
- 除非得到老师的特别许可，否则我不会将USB驱动器（也称为闪存驱动器、拇指驱动器、跳转驱动器、数据棒或其他名称）插入设备中。

我负责任地使用DCPS网络

- 我不会搜索、检索、保存、散布或展示基于仇恨的、淫秽的、粗俗的或含有色情内容的材料。
- 除非这是学校作业的一部分并且得到老师的允许，否则我不会搜索、检索、保存、散布或显示有关武器或非法毒品的图像或信息。
- 我不会使用DCPS网络进行任何非法或犯罪行为，其中包括但不限于帮派或成员活动、威胁他人的人身安全或计算机侵入。
- 除非这些活动与学校的课程或作业有关，并且老师或员工在监督这些活动，否则我不会访问在线游戏。
- 除非与学校作业有关，并且得到老师的允许，否则我将不会访问社交媒体、消息收发应用程序或群聊。这包括但不限于Facebook、Twitter、Instagram、TikTok、Snapchat、WhatsApp、Kik、Telegram、和Tumblr。

我对自己的语言以及如何在线对待他人负责。

- 我不会制作、展示或传播任何含有性暴露、色情、淫秽或使用猥亵性语言的图像、声音或消息或其他资料。
- 我不会发送、共享或发布带有仇恨、骚扰、贬损或歧视性质的消息来欺负、骚扰、威胁或恐吓他人。

我有责任在网上保持诚实。

- 我上网时不会为达到欺骗的目的冒充他人。这意味着我不会使用他人的账户、姓名或照片发送电子邮件、建立帐户或发布任何文字、图片或声音，以使他人相信我就是被冒充的人士。
- 我不会使用他人的登录名或密码。

我对尊重他人的在线财物负有责任。

- 未经适当引用，我不会剽窃或使用他人的作品。
- 未经许可（例如受版权保护），我不会下载他人的资料（包括书籍、音乐和音像资料）。
- 未经允许，我不会阅读、修改或删除老师或其他学生拥有的文件。
- 如果我在计算机屏幕上看到另一个人的作业，或者看到另一个学生已登录计算机，我将通知老师或员工，并等到另一个学生退出帐户后才使用该计算机。

每当我使用DCPS设备或DCPS网络在线发布任何内容时，我都有责任遵守学校的规定。

- 未经老师或员工的许可，我不会在学校网站、维克（Wiki）、博客（blog）、播客（podcast）、社交媒体帐户或讨论群上发布任何资料。
- 我不会张贴带有我的名字或任何其他识别信息的图片或录音（包括我的图片或视频）。
- 未经允许，我不会制作或发布任何人的图片、录音或录像。

我知道DCPS可能会检查我的DCPS设备、文件和帐户。

- 我知道在某些情况下，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。
- 我也知道，在某些情况下，如果满足以下条件，DCPS员工可能获准搜索我的个人媒体帐户或设备，或要求我从我的个人媒体帐户或设备中提取数据：
 - DCPS员工合理地怀疑，我正在或一直在使用该帐户或设备来违反DCPS政策（例如，防止欺凌政策），并且合理地怀疑，我的帐户或设备含有涉嫌违规的证据；或
 - 为了应对对生命或安全的急迫的威胁，必须这样做。



学生负责任地使用技术协议确认表

学生：

我已经阅读了《学生技术使用协议》，或者有人已经把协议读给我听并向我做出解释。我同意根据协议中列出的规则负责任地使用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（包括第25章）列出的后果，并且我对DCPS设备和DCPS网络的使用可能会受到限制。我知道，如果我看到或以其他方式意识到有人在使用DCPS设备或DCPS网络欺凌、恐吓、威胁、骚扰或伤害他人，我应当将此情况报告给老师或工作人员。我知道我的报告将被保密，并且DCPS不会容忍对我报告这类事件的任何报复。通过接受并拥有一台DCPS笔记本电脑，我也确认并同意以下内容：

1. DCPS拥有这台笔记本电脑，我的借用仅限于教学和学术目的，并符合《DCPS学生和员工规范使用技术和网络政策》。

DCPS会根据2016年《保护学生数字隐私法案》收集数据并监控笔记本电脑的使用情况。

2. 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所有费用。

3. 一旦DCPS向我索要这台笔记本电脑，我必须把它退还。如果DCPS向我索要这台笔记本电脑，但我未能退还，这可能会导致我的家人承担相关费用。

设备类型/ DCPS资产标签号 _____

学生姓名（工整书写） _____

学生签名 _____ 日期 _____

DCPS代表姓名（工整书写） _____

DCPS代表签名 _____ 日期 _____

家长/监护人：

我已与我的孩子阅读并讨论了《学生技术使用协议》。我知道：如果我的孩子不遵守这些规则中的任何一条，他/她可能会面临DCPS纪律处分规则和政策（包括第25章）列出的后果，并且他/她对DCPS设备和DCPS网络的使用可能会受到限制。

家长/监护人姓名（工整书写） _____

家长/监护人签名 _____ 日期 _____