圖書政策手冊

第 7000 節 屬性

標題： 學生技術可接受的使用和安全

代碼7540.03

狀態：活動

2015年7月20日通過

最後修訂日期：2021年7月19日

7540.03 - **學生技術可接受的使用和安全**

技術從根本上改變了社會中獲取、交流和傳輸資訊的方式。因此，教育工作者不斷調整他們的教學手段和方法，以及他們對待學生學習的方式，以整合互聯網上可用的龐大、多樣和獨特的資源。教育委員會提供技術資源（定義見章程0100），以支援其學生和教職員工的教育和專業需求。
對於學生而言，學區技術資源為他們提供了獲得技能和知識的機會，以便在數位世界中有效學習和富有成效地生活。董事會僅出於有限的教育目的為學生提供互聯網訪問許可權，並利用在線教育服務/應用程式來加強向學生提供的教學。學區的計算機網路和互聯網系統不作為公共訪問服務或公共論壇，董事會根據其有限的教育目的對其使用施加了合理的限制。

董事會根據符合適用的地方、州和聯邦法律、學區的教育使命以及《學生行為準則》中規定的對學生行為的明確期望的原則來規範學區技術資源的使用。
本政策及其相關管理指南和《學生行為準則》規定，當學生連接到學區計算機網路、互聯網連接和/或在線教育服務/應用程式時，或在學生在董事會擁有的財產或董事會贊助的活動中使用時，學生對學區技術資源和個人通信設備的使用（參見政策5136）。

用戶必須避免非法行為（如誹謗、誹謗、故意破壞、騷擾、盜竊、抄襲、不當訪問等）或不友善的行為（如人身攻擊、侵犯隱私、傷害性評論等）。
由於其技術資源不是無限的，董事會還制定了旨在保護這些資源的限制，例如限制頻寬、存儲空間和印表機的使用。

使用者在使用學區技術資源時沒有隱私權或期望隱私（包括但不限於使用學區的計算機網路和/或互聯網連接時的個人文件、電子郵件和在線活動記錄內容的隱私）。

首先，董事會可能無法在技術上將通過其技術資源獲得服務的訪問限制為僅獲得授權用於與課程相關的教學、學習和研究目的的服務。與過去不同的是，教育工作者和社區成員有機會審查和篩選材料，以評估它們是否適合根據已通過的指導方針和合理的選擇標準來支援和豐富課程（考慮到將接觸到這些課程的學生的不同教學需求、學習風格、能力和發展水準），
對互聯網的訪問，因為它是通往世界上任何公開可用的檔伺服器的門戶，為教室和學生打開了電子資訊資源，這些資源可能沒有被教育工作者篩選出來供不同年齡段的學生使用。

根據聯邦法律，委員會已實施技術保護措施，以防止（例如過濾或阻止）訪問淫穢、構成兒童色情和/或對未成年人有害的視覺展示/描述/材料，如《兒童互聯網保護法》所定義。根據董事會或學區管理員的判斷，可以對技術保護措施進行配置，以防止訪問被認為不適合學生訪問的其他材料。在學生使用學區技術資源的任何時候，技術保護措施都不得被禁用，如果這種禁用將停止保護人們訪問《兒童互聯網保護法》禁止的材料。任何試圖禁用技術保護措施的學生都將受到紀律處分。

董事會利用軟體和/或硬體來監控學生的在線活動，並阻止/過濾對兒童色情和其他淫穢、令人反感、不適當和/或對未成年人有害的材料。"對未成年人有害"是 1934 年《通信法》（47 U.S.C.
254（h）（7））定義的術語，是指任何圖片、圖像、圖形圖像檔或其他視覺描述：

一. 從整體上看，就未成年人而言，訴諸於對裸體、性或排泄物的淫穢興趣;

二. 以明顯令人反感的方式描繪、描述或代表適合未成年人的內容、實際或類比的性行為或性接觸、實際或類比的正常或性行為，或淫穢的生殖器展示;

三. 整體而言，對未成年人缺乏嚴肅的文學、藝術、政治或科學價值。

根據董事會或學區管理員的判斷，技術保護措施可以配置為防止訪問被認為不適合學生訪問的其他材料。在學生使用學區技術資源的任何時候，技術保護措施都不得被禁用，如果這種禁用將停止保護人們訪問《兒童互聯網保護法》禁止的材料。
任何試圖禁用技術保護措施的學生都將受到紀律處分。

如果技術保護措施不恰當地阻止了對包含適當材料的網站或在線教育服務/應用程式的訪問，則學區管理員或指定人員可以暫時或永久取消對此類網站的訪問。材料是否適當的判斷應以材料的內容和材料的預期用途為依據，而不是以技術保護措施的保護行為為依據。

地區管理員或指定人員可以禁用技術保護措施，以便出於善意研究或其他合法目的進行訪問。

家長被告知，確定的使用者可能能夠訪問董事會未授權用於教育目的的互聯網服務和/或資源。事實上，不可能保證學生不會通過互聯網獲得他們和/或他們的父母可能認為不適當、冒犯、令人反感或有爭議的資訊和通信。未成年人的父母有責任制定和傳達他們的孩子在使用互聯網時應遵循的標準。

根據聯邦法律，學生應接受以下教育：

一. 使用電子郵件、聊天室、社交媒體和其他形式的直接電子通信時的安全;

二. 在線披露個人身份資訊所固有的危險;

三. 未經授權訪問（例如，「駭客攻擊」、「收穫」、數字盜版「、」數據挖掘」等）、網路欺淩以及學生在線的其他非法或不當活動的後果;

四. 未經授權披露、使用和傳播有關未成年人的個人身份資訊。

工作人員應為學生提供有關上述技術的適當使用和在線安全的指導。此外，工作人員將監控學生在校期間的在線活動。

監控可能包括但不限於在課堂上對在線活動的視覺觀察;或使用特定的監控工具查看瀏覽器歷史記錄以及網路、伺服器和計算機日誌。

建築負責人負責提供培訓，以便其監督下的互聯網用戶瞭解本政策及其隨附的準則。董事會希望工作人員能夠為學生提供適當使用學區技術資源的指導和指導。此類培訓應包括但不限於有關適當在線行為的教育，包括在社交媒體上（包括在聊天室）上與其他人互動，以及網路欺淩意識和應對。學區技術資源的所有使用者（如果他們是未成年人，則為他們的父母）都必須在年度學生註冊過程中簽署學區技術使用表，以確認他們同意遵守本政策的條款和條件。

學生將被分配一個學校電子郵件帳戶，他們需要使用該帳戶進行所有與學校相關的電子通信，包括與教職員工、同齡人以及與他們就學校相關專案和作業進行通信的學區以外的個人和/或組織的電子通信。此外，根據教師的指示和授權，他們在註冊/註冊訪問各種在線教育服務時應使用學校分配的電子郵件帳戶，包括學生將用於教育目的的移動應用程式/應用程式。

學生在使用學區技術資源時應對良好行為負責——
即，在教室、學校走廊和其他學校場所和學校贊助的活動中，學生的行為與學生的預期相當。互聯網上的通信通常是公開的。董事會不批准任何未經本政策及其隨附指南授權或嚴格按照本政策及其隨附指南進行的技術資源使用。

學生只能使用學區技術資源來訪問或使用社交媒體，前提是這是根據其老師批准的此類使用計劃出於教育目的而進行的。

無視本政策及其隨附指南的使用者可能會被暫停或撤銷其使用許可權，並對其採取紀律處分。使用者對未經本政策及其隨附指南授權的學區技術資源的使用負有個人民事和刑事責任。

董事會指定學區管理員和建築級別管理員為管理員，負責啟動、實施和執行本政策及其隨附的指南，因為它們適用於學生使用**學區技術資源**。

修訂 12/4/17
修訂 2/28/18

法律
H.R. 4577， P.L. 106-554， 2000年《兒童互聯網保護法》
47 U.S.C. 254（h），（1），1934年通信法，經修訂
20 U.S.C. 6801 1965年《中小學教育法》F部分等，經修訂
18 U.S.C. 2256
18 U.S.C. 1460
18 U.S.C. 2246
47 C.F.R. 54.500
47 C.F.R. 54.501
47 C.F.R. 54.502
47 C.F.R. 54.503
47 C.F.R. 54.504
47 C.F.R. 54.505
47 C.F.R. 54.506
47 C.F.R. 54.507
47 C.F.R. 54.508
47 C.F.R. 54.509
47 C.F.R. 54.511
47 C.F.R. 54.513
47 C.F.R. 54.514
47 C.F.R. 54.515
47 C.F.R. 54.516
47 C.F.R. 54.517
47 C.F.R. 54.518
47 C.F.R. 54.519
47 C.F.R. 54.520
47 C.F.R. 54.522
47 C.F.R. 54.523