Technologie in Schulen: Die Sicherheit der Schüler*innen ohne Überwachung

Jede Schule trägt Verantwortung für das Wohlergehen und die Sicherheit ihrer Schüler*innen. Das Thema Schülersicherheit ist ein weit gefasster Begriff, der viele verschiedene Funktionsbereiche umfasst und weitgehend der Interpretation durch den Bezirk oder die Schule überlassen bleibt, die diese Maßnahmen zur Schülersicherheit umsetzen.

Die Schulen müssen selbst entscheiden, inwieweit sie Sicherheitsmaßnahmen ergreifen wollen - von der datenschutzfreundlichen Filterung von Inhalten ohne Datenerfassung bis hin zur Installation von Keyloggern auf den von der Schule ausgegebenen Geräten und der Überwachung aller Eingaben, Sendungen und Empfänge der Schüler*innen.

In dem Papier wird Folgendes untersucht

- Die Bedeutung von Kontrolle und Überwachung
- Die weiteren Auswirkungen der Begriffe in Bezug auf Bildung und den Schutz der Privatsphäre von Schüler*innen
- Überlegungen bei der Entwicklung von Technologiepolitiken, die den Institutionen einen Überblick geben, wenn es darum geht, fundierte Entscheidungen zu treffen, was getan werden muss.

Das Problem

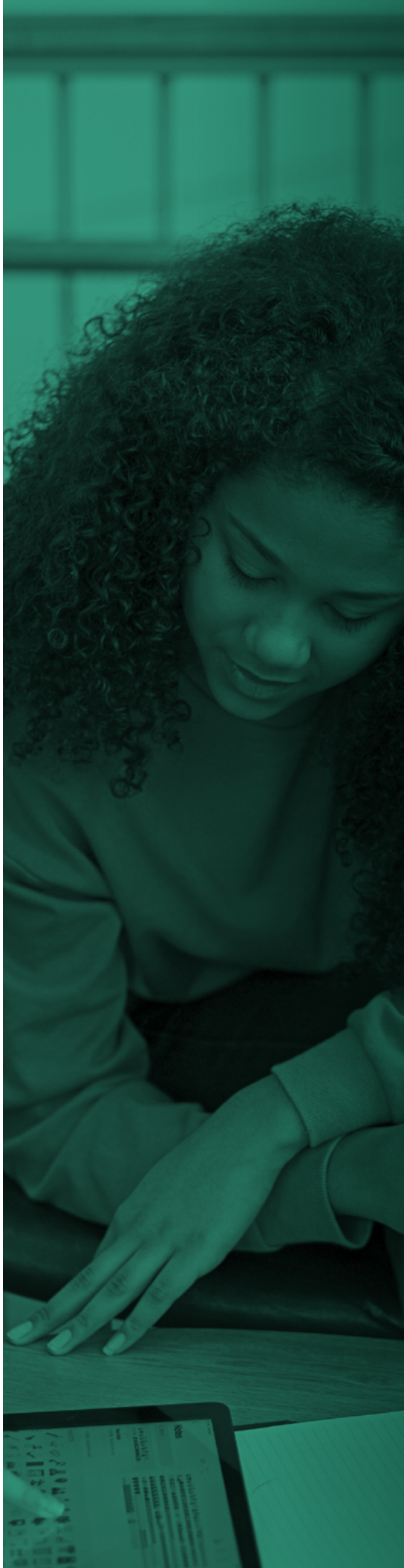
Es braucht ein ganzes Dorf: Lehrer*innen, Eltern, medizinisches Fachpersonal, Schulverwalter, Freunde… die Liste der Menschen, die das Leben der Schüler*innen beeinflussen, ist lang. Im Durchschnitt **verbringen die Schüler*innen in den Vereinigten Staaten rund tausend Stunden pro Jahr**, verteilt auf 180 Tage, in der Schule. Dadurch werden Lehrer*innen und andere Verwaltungsangestellte zu wichtigen Einflussfaktoren im Leben der Schüler*innen, die sich auf Fragen der Bildung, der psychischen Gesundheit, des Umgangs mit der Technik, des allgemeinen Wohlbefindens und darüber hinaus auswirken.

Bildungseinrichtungen gehen im Interesse der Sicherheit der Schüler*innen bei der Internetnutzung hart vor: Einige gehen sogar so weit, dass sie den Gebrauch von Schimpfwörtern, Anzeichen von möglicher Selbstverletzung oder Gewalt und Mobbing von oder gegen Gleichaltrige überprüfen. Die Ausbildung ist nur ein Teil des Lebens der Schüler*innen — und einige Schüler*innen nutzen ihre eigenen Geräte außerhalb der Aufsicht der Einrichtung, wie sollten sich die Schulen also um das geistige und körperliche Wohlbefinden der Schüler*innen kümmern? Und wie viel davon sollte von ihrer Online-Präsenz abhängen? Leider gibt es darauf keine eindeutige Antwort.

Das Internet gibt den Institutionen eine Menge Macht, um zu erziehen. Die Verfügbarkeit schülerspezifischer Bildungsansätze, unbegrenzter Informationen und unzähliger anderer Ressourcen unterstützt das Lernen der Schüler*innen in unserer informationslastigen Welt. Aber mit dieser Macht geht natürlich auch die Verantwortung einher, sich Gedanken darüber zu machen, wie Schüler*innen mit den online verfügbaren Inhalten umgehen, von denen einige unangemessen oder gefährlich sind.

Bildung geht über die Nutzung von Online-Wissen hinaus. Die Schulen wollen die Schüler*innen dazu befähigen, unabhängig und verantwortungsbewusst mit dem Internet umzugehen und gleichzeitig ihre Sicherheit zu gewährleisten. Da es keinen eindeutigen Weg gibt, diese Konzepte miteinander in Einklang zu bringen, gibt es ein breites Spektrum von Ansätzen, wenn es um die Online-Sicherheit von Schüler*innen geht. Informieren wir die Schüler*innen einfach über die sichere und angemessene Nutzung und lassen sie das Internet erkunden? Oder sperren wir das System so, dass die Schüler*innen nur auf das zugreifen können, was wir ihnen erlauben, d. h. alle Websites wurden vorab geprüft und gelten als sicher?

Diese beiden Enden des Spektrums verdeutlichen die Bandbreite der Probleme, die es im Bildungsbereich gibt: freie Entdeckungsmöglichkeiten und restriktiver Zugang. Was liegt also zwischen diesen Bereichen — was wäre, wenn wir den Schüler*innen eine gewisse Freiheit zur Erkundung einräumen, sie aber gleichzeitig im Auge behalten, damit sie nicht überfordert werden? Löst eine der beiden Seiten des Spektrums tatsächlich das Problem der Sicherheit von Schüler*innen oder gibt es bessere Alternativen? Wie können wir die Sicherheit der Schüler*innen ganzheitlich gewährleisten, auch über die Grenzen der Schulordnung hinaus?



Verschiedene Ansätze verstehen

Lassen Sie uns einige Ansätze für den Umgang mit Schülerdaten diskutieren. Die erste ist die **Überwachung.**

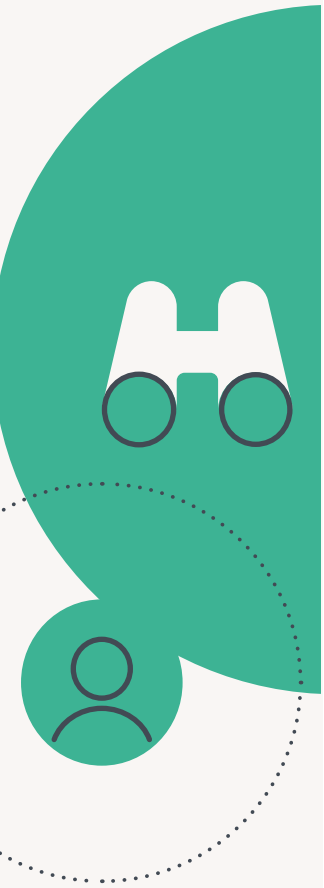
Überwachung

Bei der Überwachung der Internetnutzung von Schüler*innen werden Daten darüber gesammelt, auf welche Websites die Schüler*innen zugreifen, wann sie darauf zugreifen und wie lange sie dort bleiben. Anhand dieser Daten können die Einrichtungen ein Muster für den Zugriff auf die Daten erstellen:

- Nach welchen Arten von Material suchen die Schüler*innen?
- Zu welcher Tageszeit wird nach Inhalten gesucht? Innerhalb oder außerhalb der Schulzeit?
- Mit welchem Material verbringen die Schüler*innen die meiste Zeit?

Die Überwachung konzentriert sich auf die Daten und nicht auf die Schülerinnen und Schüler selbst, d. h. es werden eher die Websites betrachtet, auf die zugegriffen wird, als die Personen, die darauf zugreifen. Dies gibt Aufschluss über das allgemeine Verhalten einer Studentenschaft und ermöglicht es den Instituten, auf mögliche Probleme zu reagieren.

Je nachdem, wie die Daten erfasst und gespeichert werden, kann die Erfassung personenbezogener Daten (PII) reduziert werden, um die Privatsphäre der Schüler*innen zu schützen und gleichzeitig wertvolle Erkenntnisse für die Einrichtungen zu erhalten. Die Erfassung anonymer Daten kann auch den Verlust von personenbezogenen Daten bei einer Datenschutzverletzung verringern, die immer häufiger vorkommt.



Die zweite ist die **Überwachung.**

Überwachung

Die Überwachunggeht noch einen Schritt weiter, indem sie Daten mit Personen verknüpft, oft um unangemessenes Verhalten in Echtzeit zu erkennen. Dies kann so aussehen, dass der Suchverlauf einer Person aufgezeichnet wird, ihre Tastenanschläge analysiert werden oder ihre privaten Nachrichten eingesehen werden. Während einige Bezirke dies nur auf schuleigenen Geräten umsetzen, überwachen andere auch das öffentliche Verhalten von Schüler*innen **in sozialen Medien**.

Die Überwachung kann schädliches Verhalten von Schüler*innen aufdecken, bevor sie für andere oder sich selbst gefährlich werden, weshalb einige Schulbezirke diesen Ansatz verfolgen. Es kann jedoch sehr schwierig sein, dies so umzusetzen, dass die Privatsphäre der Schüler*innen nicht verletzt wird, kein **Misstrauen der Schüler*innen gegenüber ihrer Einrichtung** entsteht, keine falschen Positivmeldungen für Nicht-Bedrohungen erzeugt werden oder **bestimmte Bevölkerungsgruppen unverhältnismäßig stark betroffen sind.**

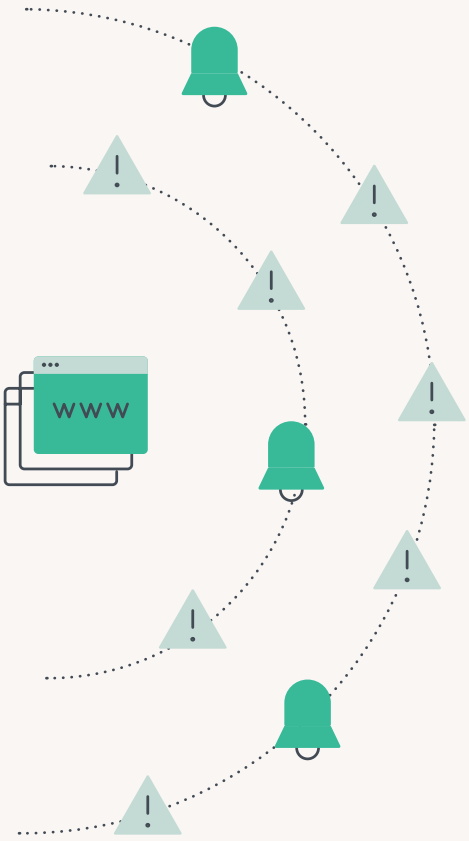
Laut einer kürzlich veröffentlichten Studie des **Center for Democracy and Technology** geben 44 % der Lehrer*innen an, dass sie einen Schüler/eine Schülerin kennen, der von den Strafverfolgungsbehörden auf der Grundlage der von ihrer Schule erhobenen Daten kontaktiert worden ist. **Und 29 % der LGBTQ+-Schüler*innen geben an**, dass sie oder jemand, den sie kennen, durch diese Technologie geoutet wurde.

Es ist nicht zu leugnen, dass sich die Überwachung auf jeden Aspekt des Lebens von Schüler*innen auswirkt, nicht nur auf die Schule. Erwachsene würden ein solches Maß an Kontrolle nicht tolerieren, sollten wir also Schüler*innen beibringen, dass dies der Status quo ist?

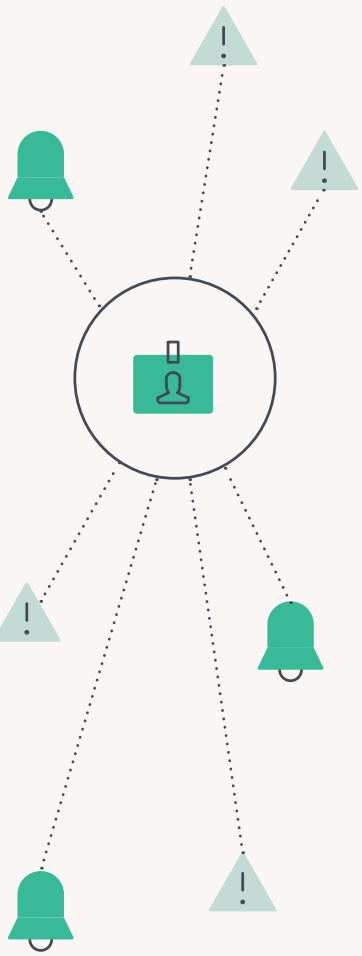
Mehr Daten, mehr Probleme

Die Erhebung und Verwendung personenbezogener Daten von Schüler*innen kann eine Reihe von Problemen aufwerfen...

Erstens besteht eine Ungleichheit in Bezug auf die Privatsphäre für Schüler*innen aus den unteren Einkommensschichten. Schüler*innen, die keinen Zugang zu einem persönlichen Gerät haben und nur das von der Schule zur Verfügung gestellte Gerät verwenden können, sind einer verstärkten Überwachung ausgesetzt. Schüler*innen mit besser verdienenden Erziehungsberechtigten haben die Möglichkeit, ihre eigenen persönlichen Geräte wie iPhone oder iPad zu verwenden, um ihre Privatsphäre zu schützen. Ein **McKinsey-Bericht aus dem Jahr 2020** , in dem die Auswirkungen des Fernunterrichts auf die Schüler*innen untersucht wurden, ergab, dass ~9 % der Schüler*innen zu Hause keinen regelmäßigen Internetzugang haben, wobei die Wahrscheinlichkeit, dass Schwarze und Hispanoamerikaner Zugang haben, um 3-4 % geringer ist. Die schleichende Ungleichheit in der Technologie kann dazu führen, dass diese Bevölkerungsgruppen anfälliger für Überwachung sind, was bedeutet, dass diese Gruppen zu ungleichen Zielen für die Folgen der Überwachung werden können.



Pädagog*innen sagen, dass Überwachungsinstrumente ihnen dabei helfen, Jugendliche zu identifizieren, die Probleme haben, und ihnen die nötige psychologische Betreuung zukommen zu lassen - und das in einer Zeit, in der Depressionen und Angstzustände bei Jugendlichen immer weiter zunehmen. Die Ergebnisse einer **landesweiten Umfrage des gemeinnützigen Center for Democracy and Technology** (CDT) deuten jedoch auf eine andere Realität hin: Anstatt Hilfe zu bekommen, werden viele Schüler*innen für Verstöße gegen die Schulregeln bestraft. Und in einigen Fällen, so lassen die Umfrageergebnisse vermuten, sind die Schüler*innen Diskriminierungen ausgesetzt. Dies wirft wiederum die Frage auf, ob die Technologie den Schüler*innen tatsächlich hilft Trotz unterschiedlicher Meinungen und Praktiken an den verschiedenen Schulen scheint eines klar zu sein: Technologie allein reicht nicht aus.



Drastische Überwachungsmaßnahmen führen zu drastischen Verbesserungen der Sicherheit, nicht wahr? Es hat sich herausgestellt, dass die Wirksamkeit der Fähigkeiten, die durch die Sammlung all dieser Daten „freigeschaltet" werden, sowohl mangelhaft ist als auch das rechtliche Risiko der Schulen erhöht, die sich dafür entscheiden, sie einzusetzen. Die Erkennungen werden anhand einer Reihe von Schlüsselwörtern implementiert, die bei Übereinstimmung eine Warnmeldung erzeugen. Diese führen zu einer enormen Anzahl von Fehlalarmen, aber die Schule ist dennoch verpflichtet, auf jeden Alarm zu reagieren.

Diese Warnungen können, wenn sie echt sind, ein Hinweis auf ein mögliches Problem mit einem Schüler/einer Schülerin sein. Aber sie sind oft nicht das erste Anzeichen von Problemen. Viel aussagekräftiger sind die Aspekte, die Menschen eher zuerst wahrnehmen — das allgemeine Verhalten, das Aussehen, die schulischen Leistungen, das Engagement für Gleichaltrige, die Stimmung, die Anwesenheit und vieles mehr. Sich auf die Technologie zu verlassen, um Schüler*innen in einer schlechten Situation aufzufangen, kann ineffektiv oder zu spät sein.

Prävention vor Inspektion

Viele Schulen wollen sicherstellen, dass die Schülerinnen und Schüler sicher im Internet surfen, indem sie den Zugang zu ungeeigneten Websites beschränken, die Material über Glücksspiele, nicht jugendfreie Inhalte, Spiele oder andere Websites enthalten, die in einem schulischen Umfeld einfach nicht angemessen sind. Die Filterung von Inhalten kann dies verhindern, indem sie den Schüler*innen den Zugang zu diesen Inhalten von vornherein verwehrt. Dieser Ansatz tendiert eher zu einem freien Internetzugang mit einem gewissen Maß an eingebauter Sicherheit. Die Einrichtungen können sich darauf verlassen, dass die Schüler*innen die Freiheit haben, sich in einem kontrollierteren Umfeld zu bewegen, das ihren Zugang zu potenziell schädlichen Inhalten einschränkt.

Wenn man weiß, dass die Inhalte gefiltert werden und schädliche Inhalte für die Schüler*innen nicht zugänglich sind, muss man möglicherweise nicht mehr überprüfen, welche Websites die Schüler*innen besuchen. Damit sind wir wieder bei der Frage des Schutzes der Privatsphäre der Schüler*innen: Sollten die Einrichtungen alles, was ein Schüler/eine Schülerin tut, überprüfen oder nur dann nachforschen, wenn dies aufgrund der Sorge um das Wohlergehen eines Schülers/einer Schülerin erforderlich ist?

Durch proaktives Sperren des Zugangs zu bestimmten Websites oder Inhaltsbereichen können Einrichtungen das Internet zur Unterstützung des Lernens und Lehrens im täglichen Unterricht nutzen, d. h. die Schüler*innen können ihr Wissen über die im Lehrplan behandelten Inhalte erweitern, ohne auf etwas zugreifen zu müssen, was sie nicht dürfen. Mit bestimmten Werkzeugen kann das Internet auf eine Handvoll zugelassener Websites beschränkt werden, oder es kann offener für zugelassene Kategorien sein. Aus der Sicht des Unterrichts bedeutet dies, dass die Lernenden auf ihre eigene Art und Weise lernen, Wissen aus verschiedenen Quellen erforschen und verstehen können, wie das Internet zu ihrem Vorteil funktioniert. Mit anderen Worten: Die Schüler*innen lernen nicht nur den für ihre Kursarbeit relevanten Stoff, sondern auch, wie man sich als guter digitaler Bürger verhält — ein wertvolles Verhalten für den Rest ihres Lebens.

Ein reaktiverer Ansatz wäre, zu analysieren, was angeschaut wird, und dann mit den Lernenden zu intervenieren, was allerdings bedeutet, dass der Inhalt bereits überwacht wurde. Dies würde bedeuten, dass jemand in der Einrichtung die Daten durchsehen müsste, um festzustellen, was geprüft wurde, um sich dann im Nachhinein damit zu befassen, was spezielles Personal und IT-Unterstützung erfordert.

Die Lösung?

Das UN-Übereinkommen über die Rechte des Kindes enthält

diese Leitlinien für den Schutz der Privatsphäre von Kindern:

1. Kein Kind darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr sowie rechtswidrigen Angriffen auf seine Ehre und seinen Ruf ausgesetzt werden.

2. Das Kind hat das Recht auf den Schutz des Gesetzes gegen solche Eingriffe oder Angriffe.

Dies ist zwar ein hervorragender Grundsatz für den Schutz der Privatsphäre von Kindern, bietet aber keine ausdrückliche Anleitung für die Umsetzung einer ausgewogenen Technologiepolitik, die die Schüler*innen vor Gefahren schützt. Schüler*innen können aufgrund ihres „Rechts auf Privatsphäre" keine Befreiung von der schulischen Überwachung auf schuleigenen Geräten beanspruchen und haben daher wenig bis keine Kontrolle darüber, wie ihre Schule mit ihren Daten umgeht. Dies kann sich sogar auf persönliche Geräte in Schulnetzen erstrecken, die den Richtlinien zur akzeptablen Nutzung (AUPs) unterliegen, die besagen, dass die Daten abgefangen werden. Mit anderen Worten: Die Studierenden haben keine Wahl, wie ihre Bildungseinrichtung ihre Daten sammelt, was insbesondere für Studierende ohne Zugang zu Datentarifen oder eigenen Geräten zu Hause gilt.

Folglich sind die Einrichtungen gezwungen, ihre eigenen Strategien und Verfahren zu entwickeln, die auf ihrer Wahrnehmung der Sicherheit der Student*innen basieren. Schließlich geht die Gefahr von einer Vielzahl von Quellen aus: Internetseiten, Gleichaltrige, sogar sie selbst. Die Schulen sind gezwungen, auf den Druck ihrer Gemeinden zu reagieren, und fühlen sich oft verpflichtet, den schlimmsten Fall - den Verlust eines Schülers/einer Schülerin - zu verhindern.

Technologie ist kein Allheilmittel

Es stellt sich also die Frage, was die Schulen tatsächlich tun sollten Auch hier gilt: Es braucht ein ganzes Dorf, und die Technik allein kann die Sicherheit der Schüler*innen nicht gewährleisten. Die Schülerinnen und Schüler müssen sich mit den Inhalten im Internet, den Beziehungen zu ihrer Familie und ihren Freunden, ihrer eigenen psychischen Gesundheit und Identität sowie ihrer Lebenssituation zu Hause auseinandersetzen. Schulberater*innen, Lehrer*innen, Angehörige der Gesundheitsberufe und Schulverwalter müssen nach wie vor kritische Beziehungen zu den Schüler*innen unterhalten, um das Wohlbefinden der Schüler*innen zu ermitteln. Die Technologie sollte nur ein Teil der Lösung sein und nicht das gesamte Leben der Schüler*innen übernehmen. Eine Überwachung sollte dann in Betracht gezogen werden, wenn es notwendig ist, einen Schüler/eine Schülerin, der von Fachleuten als Risiko eingestuft wurde, genau zu untersuchen, und nicht als Standard für die gesamte Schülerschaft. Schließlich steht den Studierenden nach ihrem Abschluss das gesamte Internet zur Verfügung. Werden die Studierenden auf die Bedrohungen des Internets vorbereitet sein, wenn die Institutionen das Netz abriegeln?

Eine gute Inhaltsfilterung kann Ablenkungen und Gefahren begrenzen, solange die Schüler*innen noch in der Schule sind, ohne dass sie das Gefühl haben, dass alles, was sie sagen, tun oder denken, auf Fehlverhalten (und damit auf Bestrafung) überprüft wird. Und bei der Filterung von Inhalten auf Ihren Schulnetzwerken und -geräten spielt das Familieneinkommen oder die demografische Herkunft der Schüler*innen keine Rolle, wodurch die Ungleichheiten, denen bestimmte Gruppen ausgesetzt sind, verringert werden.

Neben der Filterung von Inhalten sollten die Schulen auch bewährte Verfahren der Cybersicherheit anwenden, um die gesammelten Daten zu schützen. Dazu gehören:

- Klare Kontovergabe und Zugangskontrollen für Studentenkonten
- Strenge Zugangskontrollen für alle Geräte und Apps, die Zugang zu Schülerdaten haben
- Entwicklung eines klaren Plans für den Fall eines Cyberangriffs
- Sicherung von Endgeräten mit Endpoint Detection and Response (EDR)-Software
- Regelmäßige Datensicherungen für den Fall einer Wiederherstellung
- Verschlüsselung Ihrer Datenserver und -geräte
- Implementierung von Software für die Verwaltung von Sicherheitsinformationen und Ereignissen (SIEM)
- Entwicklung eines geeigneten Schulungsprogramms, um Lehrkräfte, Mitarbeiter*innen und Student*innen über die Risiken einer Online-Präsenz zu unterrichten

Die wichtigsten Erkenntnisse

- Schulen sind dafür verantwortlich, Schüler*innen vor schädlichen Internetinhalten zu schützen, aber es ist nicht klar, wie genau die Aktivitäten der Schüler*innen überprüft werden sollten
- Die Beobachtung von allem, was Schüler online*innen tun, kann negative Auswirkungen auf ihr Wohlbefinden haben
- Schulische Überwachungsprogramme können bestimmte Gruppen von Schüler*innen diskriminieren
- Durch die Beobachtung der Veranlagung eines Schülers/einer Schülerin können problematische Schüler*innen auf eine Weise erkannt werden, wie es die Technik nicht kann
- Die Überwachung und Kontrolle sollte als Teillösung für die Sicherheit der Schüler*innen sorgfältig durchgeführt werden
- Die Einrichtungen sollten strenge Sicherheitsrichtlinien entwickeln, um die Daten der Studierenden zu schützen

Wenn Sie wissen möchten, wie Jamf Teil Ihrer Technologie-, Sicherheits-, und Content-Filtering-Lösung sein kann, erfahren Sie mehr unter Jamf.com/de

Erfahren Sie mehr