



Apple im Bildungsbereich

Überblick Datenschutz und Privatsphäre für Schulen

Bildung war Apple schon immer wichtig. Wir glauben, dass moderne Technik jeden Unterricht verbessern und jeden Schüler motivieren kann. Unsere Produkte erweitern die Möglichkeiten, wie Lehrer unterrichten und Schüler lernen können – mit Zugang zu leistungsstarken Apps und fesselnden Inhalten auf den Geräten, die sie gern benutzen. Wir wissen außerdem, wie wichtig Sicherheit und Datenschutz sind, um die Daten zu schützen, die Schüler beim Lernen erstellen, speichern und verwenden.

Sicherheit und Datenschutz haben oberste Priorität beim Design all unserer Hardware, Software und Services. Mit unserem integrierten Ansatz stellen wir sicher, dass jeder Aspekt der Lernerfahrung auf einer Grundlage aufbaut, die Sicherheit und Datenschutz garantiert. Dieser Ansatz berücksichtigt den Schutz der Daten und die Sicherheit aller Benutzer in einem Bildungskontext – Lehrer, Dozenten, Mitarbeiter und Schüler.

Wir haben außerdem Features und Services speziell für den Bildungsbereich entwickelt, wie den Apple School Manager, verwaltete Apple IDs und das geteilte iPad. Diese Funktionen wurden mit dem gleichen integrierten Ansatz entwickelt und berücksichtigen zusätzlich die spezifischen Sicherheits- und Datenschutzanforderungen von Schülern und Bildungseinrichtungen.

Dieser Überblick beschreibt, wie verwaltete Apple IDs und unsere Bildungsfeatures und -services den Datenschutz und die Sicherheit der Schüler behandeln. Sie können diesen Überblick verwenden, um mit Eltern darüber zu sprechen, wie die Daten ihrer Schüler von Apple geschützt werden.

Apples Engagement für den Schutz der Daten der Schüler

Apple wird niemals Daten von Schülern für Werbung oder Marketingzwecke sammeln, teilen oder verkaufen. Wir erstellen auch keine Schülerprofile basierend auf den Inhalten ihrer E-Mails oder ihrem Surfverhalten. Außerdem werden wir persönliche Schülerdaten außer zum Anbieten von Bildungsservices weder erfassen, verwenden noch offenlegen. Apple wird persönliche Schülerdaten nicht verkaufen oder zum gezielten Einsatz von Werbung bei Schülern offenlegen.

Als weiteren Beweis für unser Engagement hat Apple eine Apple Datenschutzrichtlinie erstellt, die gemeinsam mit dem Apple School Manager Vertrag regelt, wie wir Benutzerdaten erfassen, verwenden, offenlegen, übertragen und speichern. Außerdem haben wir die Student Privacy Pledge unterzeichnet.

Apple School Manager und verwaltete Apple IDs

Apple bietet Bildungseinrichtungen aller Größen Services für die einfache Implementierung von iPad und Mac. Diese Services wurden unter Sicherheits- und Datenschutzaspekten entwickelt, sodass Ihre Einrichtung und die Daten der Schüler vor, während und nach der Implementierung geschützt sind.

Der Apple School Manager ist ein kostenfreier, webbasierter Service, der Technologiemanagern alles bietet, was sie brauchen, um iPad und Mac in Schulen zu implementieren. Mit Apple School Manager können Sie Inhalte kaufen, die automatische Geräteregistrierung bei Ihrer MDM-Lösung (Mobile Device Management) konfigurieren, Accounts für Schüler und Mitarbeiter erstellen und iTunes U Kurse einrichten.

Eine zentrale Funktion von Apple School Manager ist die Möglichkeit, verwaltete Apple IDs zu erstellen, die der Kontrolle durch die Bildungseinrichtung unterliegen. Verwaltete Apple IDs sind eine neue Art Apple ID, mit denen Schüler auf iCloud, iTunes U und geteilte iPads zugreifen können, während die Schule die nötige Kontrolle behält. Verwaltete Apple IDs wurden ausschließlich für den Bildungsbereich entwickelt.

Um sicherzustellen, dass die für die Schüler bereitgestellten Geräte der Schulen nur für Bildungszwecke verwendet werden können, haben wir bestimmte Features und Funktionen für verwaltete Apple IDs deaktiviert. Schüler können nicht beliebige Inhalte im App Store, iBooks Store oder iTunes Store erwerben. Apple Pay, Meine Freunde suchen, Mein iPhone suchen, iCloud Mail, HomeKit und iCloud Schlüsselbund sind ebenfalls deaktiviert. FaceTime und iMessage sind ebenfalls standardmäßig deaktiviert, können aber von einem Administrator aktiviert werden.

Mit Apple School Manager können automatisch für alle Schüler und Mitarbeiter verwaltete Apple IDs erstellt werden. Die nötigen Daten dafür werden aus dem jeweiligen Management-Informationssystem (MIS) übernommen oder aus CSV Dateien, die aus dem Verzeichnisdienst der Schule exportiert werden können. Die einzelnen Benutzeraccounts werden basierend auf Daten erstellt, die aus der Quelle ausgelesen werden und schreibgeschützt sind. Zusätzliche Informationen, wie die Kennung der verwalteten Apple ID und das dazugehörige Passwort, werden zu den Accountinformationen im Apple School Manager hinzugefügt. Es werden keine Daten zurück ins MIS geschrieben.

Mit jedem Benutzeraccount können die folgenden Daten verknüpft sein, die in der Accountauflistung oder bei der Auswahl eines Accounts einsehbar sind:

- Eine alphanumerische ID, die für diesen Account eindeutig ist
- Vorname, zweiter Vorname und Nachname
- Klassenstufe, sofern angegeben
- Kursanmeldungen
- E-Mail Adresse, sofern angegeben
- Rolle
- Standort
- Quelle
- Erstellungsdatum
- Änderungsdatum

Da verwaltete Apple IDs von der Schule erstellt und zugewiesen werden, können ganz einfach Passwörter zurückgesetzt, Accounts geprüft und Rollen für jede Person im Schulbezirk erstellt werden. Jedes Mal, wenn ein Account von einem Administrator geprüft oder das Passwort zurückgesetzt wird, zeichnet Apple School Manager die Aktivität in einem Protokoll auf.

Verwaltete Apple IDs unterstützen außerdem verschiedene Codeoptionen, von einfachen vierstelligen Codes bis hin zu komplexen alphanumerischen Passwörtern. Für Accounts, die erstmalig importiert oder erstellt werden, erstellt Apple School Manager temporäre Passwörter. Mit diesen temporären Passwörtern melden sich die Benutzer der Accounts zum ersten Mal mit ihrer verwalteten Apple ID an. Dabei müssen Sie ihr Passwort ändern. Apple School Manager zeigt das von den Schülern gewählte Passwort niemals an, sobald es das temporäre Passwort ersetzt hat. Ein Schüler kann sich für den Zugriff auf seine Schularbeit an einem Gerät anmelden, das nicht von der Einrichtung verwaltet wird, wie z. B. an einem Gerät bei ihm zuhause. Er verwendet dafür seine verwaltete Apple ID, das Passwort und einen sechsstelligen Bestätigungscode, der ihm vom Administrator über Apple School Manager gegeben wird. Dieser zusätzliche Bestätigungscode verfällt nach einem Jahr.

Ein Apple School Manager Administrator kann einen verwalteten Apple ID Account freigeben. Danach ist er für Schüler, Lehrer, Mitarbeiter oder Manager noch etwa 180 Tage zugänglich. Anschließend werden alle Daten, die zum Account gehören, unwiederbringlich gelöscht. Sollte eine Einrichtung die sofortige Löschung einer verwalteten Apple ID verlangen, ist der Account nicht länger zugänglich und alle Daten, die zur ID gehören, werden innerhalb von 40 Tagen unwiederbringlich gelöscht.

Verwaltete Apple IDs und geteiltes iPad

In Fällen, in denen sich Schüler ein iPad teilen, bietet Apple den Schülern die Möglichkeit, sich mit einer verwalteten Apple ID anzumelden, um schnell auf ihre eigenen Apps, Inhalte und Einstellungen zuzugreifen und mit ihnen zu arbeiten. So können mehrere Schüler das gleiche iPad benutzen, und gleichzeitig wird für jeden Schüler eine individuelle Lernerfahrung sichergestellt.

Wenn sich ein Schüler beim geteilten iPad anmeldet, wird die verwaltete Apple ID automatisch bei den Identitätsservern von Apple authentifiziert. Wenn der Schüler das Gerät vorher noch nicht verwendet hat, werden ein neuer Benutzerordner und Schlüsselbund für den Benutzer bereitgestellt. Nachdem der lokale Account des Schülers erstellt und entsperrt wurde, meldet sich das Gerät automatisch bei iCloud an. Als Nächstes werden die Einstellungen des Schülers wiederhergestellt und seine Daten von iCloud synchronisiert.

Während die Sitzung des Schülers aktiv und das Gerät online ist, werden erstellte und veränderte Dokumente und Daten in iCloud gespeichert. Und ein Synchronisierungsmechanismus im Hintergrund sorgt dafür, dass Änderungen in iCloud gesichert werden, nachdem der Schüler sich abgemeldet hat.

iCloud und Datensicherheit

Wenn Schüler Dokumente erstellen, im Unterricht interagieren und an Klassenzimmeraktivitäten teilnehmen, ist es wichtig, dass sie ihre Daten sicher speichern können und diese jederzeit geschützt sind – auf dem Gerät und in iCloud.

Mit iCloud können Benutzer ihre Dokumente, Kontakte, Notizen, Lesezeichen, Kalenderereignisse und Erinnerungen automatisch speichern lassen. So können sie auf iOS und Mac sowie über iCloud.com auf Mac oder PC auf ihre Daten zugreifen. Wenn sich der Benutzer bei iCloud anmeldet, erhalten Apps standardmäßig Zugriff auf iCloud Drive. Benutzer können den Zugriff der einzelnen Apps in Einstellungen unter iCloud steuern. Verwaltete Apple IDs sind standardmäßig für die obigen Services aktiviert.

iCloud arbeitet mit branchenüblichen Sicherheitspraktiken und wendet strenge Richtlinien zum Datenschutz an. iCloud schützt die Benutzerdaten, indem sie verschlüsselt über das Internet gesendet und in verschlüsseltem Format auf dem Server abgelegt werden. Außerdem verwendet es sichere Tokens zur Authentifizierung. Das bedeutet, dass Schülerdaten sowohl bei der Übertragung als auch als ruhende Daten in iCloud vor unbefugtem Zugriff geschützt sind. iCloud verwendet mindestens eine 128-Bit AES-Verschlüsselung – das ist das gleiche Sicherheitsniveau, wie es große Finanzinstitute einsetzen – und gibt den Verschlüsselungsschlüssel niemals an Dritte heraus. Apple speichert die Verschlüsselungsschlüssel in eigenen Rechenzentren. iCloud speichert Passwörter und Anmeldedaten der Schüler so, dass Apple sie weder lesen, noch auf sie zugreifen kann.

Weitere Informationen über iCloud Sicherheit und Datenschutz gibt es unter <https://support.apple.com/de-de/HT202303>.

CloudKit und Apps von anderen Anbietern

Apps von anderen Anbietern sind ein wesentlicher Teil einer modernen Lernumgebung. Um Schülern in Apps von anderen Anbietern das gleiche reibungslose Erlebnis der Datenspeicherung und des Datenzugriffs zu ermöglichen, haben wir CloudKit entwickelt – ein Framework, mit dem Entwickler anderer Anbieter Daten in iCloud speichern und synchronisieren können.

Wenn Schüler eine App nutzen, die CloudKit verwendet, werden sie automatisch mit ihrer Apple ID angemeldet. Sie müssen weder einen neuen Account erstellen noch irgendwelche anderen persönlichen Daten preisgeben. Sie haben immer Zugriff auf die aktuellsten Informationen in der App, ohne dass sie sich Passwörter oder Benutzernamen merken müssen. Entwickler haben keinen Zugriff auf die Apple ID der Schüler, sondern nur auf eine eindeutige Kennung.

Unabhängig davon, ob der Entwickler CloudKit verwendet oder nicht, ist es wichtig, sich darüber bewusst zu sein, dass Apps von anderen Anbietern Informationen über die Schüler sammeln können. Es liegt in

der Verantwortung Ihrer Schule, sicherzustellen, dass alle einschlägigen Gesetze eingehalten werden, wenn Sie Apps von anderen Anbietern verwenden. Ihre Schule sollte die Nutzungsbedingungen, Richtlinien und Praktiken von Apps von anderen Anbietern prüfen, um zu verstehen, welche Daten diese über Schüler erheben können, wie diese Daten verwendet werden und ob ein Einverständnis der Eltern erforderlich ist.

Wir verlangen von den Entwicklern von Apps im App Store, dass sie unseren besonderen Richtlinien zustimmen, die mit dem Ziel erstellt wurden, unsere Benutzer und ihre Daten zu schützen. Wenn wir von einer App erfahren, die gegen diese Richtlinien verstößt, muss der Entwickler das Problem lösen oder die App wird aus dem App Store entfernt.

Ortungsdienste und der Modus „Verloren“

Bei der Verwendung von Apps und Services auf ihrem Gerät werden Schüler wahrscheinlich aufgefordert, die Ortungsdienste zu aktivieren, je nach App oder Aktivität in der App. Apple bietet den Benutzern eine fein abgestimmte Kontrolle darüber, wie ihre Standortinformationen verwaltet und mit Apps und Clouddiensten geteilt werden.

Ortungsdienste gestatten standortbasierten Apps, wie Karten, Wetter und Kamera, das Erfassen von Standortinformationen. Die Standortinformationen, die von Apple erfasst werden, werden nicht auf eine Weise gespeichert, die den Schüler persönlich identifizierbar macht. Standortdienste sind standardmäßig deaktiviert und können durch das Bedienen eines einzigen Schalters in den Einstellungen aktiviert werden. Die Schüler können den Zugriff für jede App einzeln gestatten, die um die Nutzung des Dienstes bittet.

Wenn eine App auf dem iPad Ortungsdienste verwendet, erscheint ein Pfeilsymbol in der Menüleiste. Apps können den dauerhaften Erhalt von Standortinformationen anfordern oder Standortinformationen nur benutzen, während die App verwendet wird. Benutzer können sich dafür entscheiden, diesen Zugriff nicht zu gestatten und ihre Entscheidung in den Einstellungen ändern. Der Zugriff kann niemals gestattet werden, bei Verwendung gestattet werden oder immer gestattet werden, je nach angefragter Standortverwendung der App. Wenn Apps Zugriff auf den Standort gestattet ist und die Apps davon im Hintergrund Gebrauch machen, werden Benutzer an ihre Zustimmung erinnert und können den Zugriff der App ändern.

Ortungsdienste werden auch verwendet, um Ihrer Schule beim Wiederfinden eines gestohlenen oder verlorenen Gerätes zu helfen. Auf einem betreuten Gerät mit iOS 9.3 oder neuer kann ein MDM-Administrator den Modus „Verloren“ per Fernzugriff aktivieren. Wenn der Modus „Verloren“ aktiviert ist, wird der aktuelle Benutzer abgemeldet und das Gerät kann nicht entsperrt werden. Auf dem Display erscheint eine Nachricht, die vom Administrator angepasst werden kann, wie z. B. die Anzeige einer Telefonnummer, die angerufen werden soll, wenn das Gerät gefunden wird. Wenn auf dem Gerät der Modus „Verloren“ aktiviert ist, kann der Administrator das Gerät auffordern, seinen aktuellen Standort an den MDM-Server zu senden. Auch wenn ein Administrator den Modus „Verloren“ bei einem Gerät deaktiviert, wird der Gerätestandort ebenfalls gesendet und der Benutzer über diesen Vorgang informiert.

Diagnosedaten

Wenn Sie und Ihre Schüler uns dabei unterstützen möchten, können Sie an unserem Diagnose- & Nutzungsprogramm teilnehmen und anonymisierte Daten zu Ihrem Gerät und Ihren Apps an Apple senden.

Dafür ist eine ausdrückliche Zustimmung erforderlich. Benutzer können die Daten auf ihrem Gerät anzeigen oder jederzeit das Senden der Daten in den Einstellungen beenden. Bei Implementierungen mit geteiltem iPad kann die Schule das Einreichen der Diagnose- und Nutzungsdaten einschränken.

iOS verfügt außerdem über erweiterte Diagnosefähigkeiten, die beim Debugging oder Beheben von Problemen mit dem Gerät nützlich sein können. Diese erweiterten Diagnosefähigkeiten senden ohne zusätzliche Tools und ausdrückliche Zustimmung keine Daten an Apple.

Internationaler Datentransfer

Apple arbeitet zusammen mit Schulen auf der ganzen Welt daran, die besten Lerntools für Lehrer und den Unterricht zur Verfügung zu stellen.

Mit Apple School Manager, verwalteten Apple IDs, iTunes U und iCloud können persönliche Daten in einem anderen Land als dem Ursprungsland gespeichert werden. Wo auch immer die Daten gespeichert werden, sie unterliegen den gleichen strengen Datenspeicherungsstandards und -anforderungen.

Apple stellt sicher, dass persönliche Daten, die aus dem Europäischen Wirtschaftsraum oder der Schweiz an die Vereinigten Staaten von Amerika übermittelt werden, entweder von einem geltenden Safe Harbor Programm oder seinem Nachfolger geregelt werden, für das Apple Inc. zertifiziert ist, oder den Model Contractual Clauses/ Swiss Transborder Data Flow Agreement unterliegen, die dem Apple School Manager Vertrag angehängt sind.

Weitere Ressourcen

Das Vertrauen Ihrer Schule und Ihrer Schüler bedeutet für Apple alles. Deshalb respektieren wir die Privatsphäre der Schüler und schützen sie durch strikte Richtlinien, die den Umgang mit allen Daten regeln.

In den folgenden zusätzlichen Ressourcen finden Sie weitere Informationen. Wenn Sie Fragen zum Datenschutz haben, können Sie uns jederzeit direkt unter www.apple.com/de/privacy/contact erreichen.

Apples Engagement für den Schutz Ihrer Daten: www.apple.com/de/privacy/

Apple Bildung: IT & Implementierung www.apple.com/de/education/it/

Apple School Manager Vertrag: www.apple.com/legal/education/apple-school-manager/

Hilfe zu Apple School Manager: help.apple.com/schoolmanager/

Implementierungsreferenz für den Bildungsbereich: help.apple.com/deployment/education/

iOS Sicherheitsleitfaden: www.apple.com/de/business/docs/iOS_Security_Guide.pdf



© 2016 Apple Inc. Alle Rechte vorbehalten. Apple, das Apple Logo, Apple Pay, FaceTime, iMessage, iPad, iTunes U, Mac, Siri, Spotlight und Touch ID sind Marken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. HomeKit ist eine Marke der Apple Inc. iCloud und iTunes Store sind Dienstleistungsmarken der Apple Inc., die in den USA und weiteren Ländern eingetragen sind. Der App Store ist eine Dienstleistungsmarke der Apple Inc. IOS ist eine Marke oder eingetragene Marke von Cisco in den USA und weiteren Ländern und wird unter Lizenz verwendet. Andere hier genannte Produkt- und Herstellernamen sind möglicherweise Marken ihrer jeweiligen Rechtsinhaber. Änderungen der Produktspezifikationen vorbehalten. Mai 2016

