Apple im Bildungsbereich
Elternleitfaden für Datenschutz

Dieser Leitfaden soll Eltern und Erziehungsberechtigten veranschaulichen, wie Apple dazu beiträgt, den Schutz vonSchülerdaten zu gewährleisten. Wir haben das Ziel, die besten Lernwerkzeuge zur Verfügung zu stellen und dabei dafür zu sorgen, dass unsere Technologien die Privatsphäre von Schülern und ihre Daten schützen. Datenschutz und Sicherheit sind ein wichtiger Bestandteil bei der Entwicklung von Apple Hardware, Software und Diensten. Hinsichtlich Schülerdaten arbeiten wir mit den folgenden Richtlinien:

- Wir verkaufen keine Daten von Schülern und teilen sie niemals mit anderen Unternehmen, die sie für Marketing- oder Werbezwecke nutzen möchten.
- Wir erstellen auch keine Schülerprofile auf Basis der Inhalte ihrer E–Mails oder ihres Surfverhaltens.
- Persönliche Daten von Schülern werden von uns nicht gesammelt, ausgewertet oder weitergegeben, außer zur Bereitstellung relevanter Bildungsdienste.

Unabhängig davon, ob Ihre Schule ein iPad oder einen Mac bereitstellt oder Ihre Schüler ein eigenes Gerät mit in die Schule bringen, bietet Ihnen dieser Leitfaden Informationen zum Datenschutz hinsichtlich der folgenden bildungsrelevanten Kategorien:

- **Schüler-Accounts** – Eine ID von Apple, mit der Ihre Schüler Zugang zu Diensten und anderen Lernmaterialien erhalten.
- **Schülerdaten** – Daten, die über Ihre Schüler gespeichert werden und Daten, die Schüler bei der Arbeit mit digitalen Technologien erstellen.
- **Geräteverwaltung** – Die Art und Weise, auf die Schulen iPad und Mac einrichten und verwalten, um eine produktive Lernumgebung zu ermöglichen.
- **Digitale Kompetenz** – Best Practices zur Nutzung von Technologien in der Schule und zu Hause.

Schüler-Accounts

iPad und Mac sind wie das Schließfach, der Schreibtisch oder der Laborplatz von Schülern in Einem – ein Ort, an dem alle ihre Materialien und Schularbeiten sofort zugänglich sind. Schüler können zum Beispiel auf dem iPad oder Mac lesen und Notizen machen oder multimediale Projekte erstellen, um ein naturwissenschaftliches Experiment zu dokumentieren. Um Arbeiten zu speichern oder auf andere Apple Ressourcen zugreifen zu können, benötigen Ihre Schüler einen Account bei Apple. Es gibt zwei Arten von Accounts – individuelle Accounts, auch Apple ID genannt, und für Schulen entwickelte Accounts, die sogenannten verwalteten Apple IDs. In diesem Leitfaden liegt der Fokus auf verwalteten Apple IDs.

Verwaltete Apple IDs

Anders als individuelle Apple IDs von Benutzern sind verwaltete Apple IDs Eigentum der Einrichtung oder des Schulbezirks und werden auch von ihnen verwaltet. Sie wurden speziell für die Anforderungen von Bildungseinrichtungen entwickelt, unter anderem für die Einschränkung von Käufen und Kommunikation. Mit einer verwalteten Apple ID kann sich der Schüler an seinem iPad oder Mac anmelden und auf Apple Dienste wie iCloud, den Cloud-Dienst von Apple, und iTunes U zugreifen. Bei verwalteten Apple IDs sind einige Dienste wie Apple Pay, HomeKit und „Mein iPhone suchen“ deaktiviert. Mit verwalteten Apple IDs können Schüler außerdem keine Käufe im App Store, im iTunes Store, oder auf Apple Music machen.

Schulen können verwaltete Apple IDs für Schüler erstellen und gleichzeitig Datenschutz und Sicherheit gewährleisten. In diese IDs ist eine weitverbreitete Sicherheitsmaßnahme integriert: die zweistufige Authentifizierung. Um den Datenschutz bei Schülern zu gewährleisten, wird in den verwalteten IDs eine beschränkte Anzahl an Schülerdaten gespeichert. Bei der Erstellung eines Accounts sind zum Beispiel die mit einer verwalteten Apple ID verbundenen Daten auf den Namen des Schülers, die Jahrgangsstufe, die Klasse und die Schüler-ID beschränkt. (Die Schule kann optional die E-Mail-Adresse oder ein Foto des

Schülers verwenden.) Andere Schülerdaten werden separat im Schülerinformationssystem (SIS) der Schule gespeichert.

Verwaltete Apple IDs können auch für Schulaufgaben mit einem privaten iPad oder Mac verwendet werden. Um ihre Hausaufgaben zu machen, können sich Schüler mit ihrer verwalteten Apple ID bei iCloud anmelden und ein Passwort für die Nutzung zu Hause verwenden, das von der Schule für die zweistufige Authentifizierung vergeben wurde. Selbst wenn Schüler zu Hause eine verwaltete Apple ID auf einem privaten Gerät benutzen, kann die Schule die Nutzung von Features wie FaceTime oder iMessage einschränken. Hinweis: iCloud Dokumente, die von Schülern während der Anmeldung mit ihrer verwalteten Apple ID erstellt wurden, unterliegen ebenfalls einer Überprüfung, wie unten beschrieben.

Verwaltete Apple IDs sind für die Nutzung an der Schule gedacht. Außerhalb der Schule können Schüler ab 13 Jahren, abhängig von den gesetzlichen Bestimmungen, auf die kommerziellen Angebote von Apple zugreifen, indem sie eine persönliche Apple ID erstellen. Schüler unter 13 Jahren können eine Apple ID als Familienmitglied mit der Familienfreigabe nutzen.

Wenn eine Schule es für angemessen hält, dass sich Schüler an einem von der Schule verwalteten Gerät mit einer persönlichen Apple ID anmelden, fällt die Verwendung dieser persönlichen Apple ID unter die Datenschutzrichtlinie und zusätzlichen Nutzungsbestimmungen von Apple. Die Schule sollte daher sicherstellen, dass die Nutzung einer persönlichen Apple ID nach geltenden nationalen Gesetzen und Schulrichtlinien zulässig ist.

Verwaltete Apple IDs überprüfen

Bei verwalteten Apple IDs besteht die Möglichkeit, im Ermessen der Schule den Account eines Schülers zu überprüfen. Dieses Feature folgt strengen Vorschriften, in deren Rahmen alle Überprüfungen protokolliert werden. Bei Überprüfungen werden einem Administrator, der Verwaltung oder einem Lehrer Überprüfungsprivilegien im Apple School Manager, dem IT-Portal von Apple, gewährt. Wenn ein Account von der Schule überprüft wird, wird diese Überprüfung protokolliert und mit einem Zeitstempel und den Anmeldeinformationen des Prüfers versehen. Während des Überprüfungszeitraums kann der Prüfer in iCloud gespeicherte Inhalte des Nutzers lesen und ändern. Dies gilt auch für Apps, die Daten in iCloud speichern. Die Berechtigung zur Überprüfung läuft nach sieben Tagen ab. Falls nötig, können sich Eltern mit ihrer Schulverwaltung abstimmen, um den Account eines Schülers zu prüfen.

Kommunikation: SMS, E-Mail, Sprach/Video-Chat

Verwaltete Apple IDs können nicht für E-Mails genutzt werden. Die Nachrichten- und Videochat-Dienste von Apple, iMessage und FaceTime, sind standardmäßig deaktiviert. Schulen können diese Features nach eigenem Ermessen aktivieren. Sie unterliegen dann den Bestimmungen für diese Features. Um sich über die Richtlinien Ihrer Schule zu E-Mails und elektronischer Kommunikation zu informieren, bitten Sie Ihre Schulleitung um eine Kopie der Schulrichtlinien.

Schülerdaten

Heutzutage können Schüler Notizen und Skizzen erstellen, verschlüsseln, animieren, aufzeichnen, veröffentlichen und Aufgaben auf dem iPad und Mac erledigen. Um sicherzustellen, dass die Daten des Schülers stets privat und sicher sind, verarbeitet Apple Daten mit einem Datenminimierungsansatz. In den folgenden Abschnitten sind Beispiele dafür genannt, wie Schülerdaten in Bezug auf Standort, Sicherheit, Eigentum, kommerzielle Aktivitäten und Compliance gehandhabt werden können.

Standortdaten

Mit Ortungsdiensten können Standortdaten von standortbasierten Apps und Websites verwendet werden. Zum Beispiel kann es vorkommen, dass Schüler im naturwissenschaftlichen Unterricht oder bei einer Exkursion Vogelarten auf der ganzen Welt kartieren müssen. Wenn Schüler ihr Gerät zum ersten Mal einrichten, können sie die Ortungsdienste im Systemassistenten aktivieren. Über die MDM-Lösung (Mobile Device Management) Ihrer Schule können Sie diese Auswahl für Geräte, die Schuleigentum sind, ausblenden und die Ortungsdienste standardmäßig deaktivieren. Apple ermöglicht eine genaue Kontrolle

darüber, wie Standortdaten in einzelnen Apps verwendet werden. Diese Einstellungen können vom Schüler auf *niemals gestattet*, *bei Verwendung gestattet* oder *immer gestattet* gesetzt werden.

Bei der Benutzung ihrer Geräte werden Schüler wahrscheinlich durch verschiedene Apps dazu aufgefordert, die Ortungsdienste zu aktivieren. Wenn Schüler einer App gestattet haben, immer auf Ortungsdienste zuzugreifen, können sie gelegentlich an ihre Auswahl erinnert werden und ihre Entscheidung jederzeit ändern.

Sicherheit auf dem Gerät und in der Cloud

Wenn Ihre Schüler Dokumente erstellen, mit Inhalten arbeiten und an Unterrichtsaktivitäten teilnehmen, ist es sehr wichtig, dass sie ihre Arbeit sicher speichern können und wissen, dass ihre Daten geschützt sind. Datenschutz und Sicherheit stehen bei unseren Diensten von Anfang an im Vordergrund. Dadurch stellen wir sicher, dass sowohl die Daten der Schüler als auch der Schule vor, während und nach der Übergabe der Geräte an Schüler geschützt sind.

In Bezug auf Daten ist es hilfreich, an zwei Bereiche zu denken: Daten auf dem Gerät und Daten, die in der Cloud gespeichert werden. Einige Schulen nutzen eventuell „Geteiltes iPad", ein Feature in iOS, das eine persönliche Lernerfahrung auf iPad Geräten bietet, die im Laufe des Tages von verschiedenen Schülern verwendet werden. Mit dem Feature „Geteiltes iPad" können Schüler ihre eigenen Arbeiten und Einstellungen mit ihrer verwalteten Apple ID in der Cloud speichern, bevor sie den Unterricht verlassen. Ihre Arbeiten werden automatisch in iCloud gespeichert. Dies erfolgt so, dass andere Schüler, die das iPad ebenfalls nutzen, nicht darauf zugreifen können.

Arbeiten von Schülern können sicher auf dem iPad oder Mac gespeichert werden, da Daten auf dem Gerät verschlüsselt werden. Die Verschlüsselung wird auf dem iPad automatisch aktiviert und kann mit FileVault auf dem Mac aktiviert werden. Das bedeutet, dass ohne das Passwort des Schülers nicht auf die Daten auf dem Gerät zugegriffen werden kann.

iCloud, der Cloud-Dienst von Apple, erfordert für das Verschieben von Daten ein sicheres Netzwerkprotokoll namens HTTPS. iCloud arbeitet mit branchenüblichen Sicherheitspraktiken und wendet strenge Richtlinien zum Datenschutz an. Auf dem iPad und dem Mac ist eine verschlüsselte Verbindung auch dann erforderlich, wenn eine Verbindung zu einem Dienst oder dem Internet hergestellt wird.

Die Cloud schützt Benutzerdaten, indem sie verschlüsselt über das Internet gesendet und in einem verschlüsselten Format auf dem Server abgelegt werden. Außerdem verwendet sie sichere Tokens zur Authentifizierung. Das bedeutet, dass Schülerdaten sowohl während der Übertragung als auch in iCloud vor unbefugtem Zugriff geschützt sind. In iCloud wird das gleiche Maß an Sicherheit genutzt, das auch von großen Finanzinstituten eingesetzt wird. Verschlüsselungsschlüssel werden nie an Dritte weitergegeben. Apple speichert die Verschlüsselungsschlüssel in eigenen Rechenzentren. iCloud speichert Passwörter und Anmeldedaten von Schülern so, dass Apple sie weder lesen, noch auf sie zugreifen kann.

Weitere Informationen über iCloud Sicherheit und Datenschutz finden Sie unter https://support.apple.com/de-de/HT202303.

Dateneigentum

Apple ist nicht Eigentümer der Daten von Schülern auf Geräten oder in der Cloud. Ihre Schule oder Ihr Bezirk kann kontrollieren, wie und wann Schüler Zugang zu Diensten und Inhalten auf ihren Geräten haben. Von Schülern erstellte Arbeiten bleiben jedoch ihr Eigentum. Weitere Informationen finden Sie in den Datenschutzrichtlinien Ihrer Schule.

Student Privacy Pledge

Das Future of Privacy Forum (FPF) und die Software & Information Industry Association (SIIA) haben einen Student Privacy Pledge eingeführt, um die Privatsphäre von Schülern sicherzustellen. Apple hat diesen Student Privacy Pledge unterzeichnet. Weitere Informationen finden Sie im Student Privacy Pledge.

Globale Compliance

Apple arbeitet mit Schulen auf der ganzen Welt zusammen, um die beste Technologie zum Lernen zur Verfügung zu stellen, und hat die ISO 27001 Datenzertifizierung erhalten. Mit Apple School Manager, verwalteten Apple IDs, iTunes U und iCloud können persönliche Daten in einem anderen Land als dem Ursprungsland gespeichert werden. Unabhängig davon, wo die Daten gespeichert werden, unterliegen sie den gleichen strengen Datenspeicherungsstandards und -anforderungen.

Geräteverwaltung

Um eine bessere Lernumgebung zu gewährleisten, wird Ihre Schule möglicherweise iPad oder Mac Geräte für Schüler sowie die darauf enthaltenen Apps und Bücher einrichten und verwalten. Mit Softwarelösungen für die Geräteverwaltung können Schulen sicherstellen, dass Richtlinien und Einstellungen auf Geräten angewandt werden. Dies gilt auch für Geräte im Eigentum von Schülern, die mit in die Schule gebracht werden. In diesem Abschnitt sehen wir uns die gängigsten Tools an, die zur Verwaltung von Geräten genutzt werden, um die Daten der Schüler zu sichern und zu schützen. Außerdem ist es wichtig zu verstehen, wessen Eigentum das iPad oder der Mac ist, der von einem Schüler verwendet wird. Dies legt nämlich fest, welche Features von der Schule verwaltet werden.

In Schulen gibt es drei grundlegende Szenarien zum Eigentumsstatus:

- **One-to-One-Implementierung**: Die Schule kauft ein iPad oder einen Mac und stellt diese ihren Schülern zur Verfügung. Diese Art der Implementierung kann für eine bestimmte Jahrgangsstufe, einen Fachbereich oder einen gesamten Bezirk oder eine Universität erfolgen.
- **Implementierung mit geteilter Nutzung**: Die Schule kauft und verteilt mehrere iPad oder Mac, die von den Schülern abwechselnd genutzt werden.
- **Implementierung mit Nutzung eigener Geräte** (BYOD): Sie kaufen ein iPad oder einen Mac für Ihren Schüler, das oder den er an der Schule oder Universität nutzen kann.

Geräte verwalten

Das Gerät Ihres Schülers kann durch eine MDM-Lösung (Mobile Device Management) verwaltet werden, d. h. durch einen Dienst eines Drittanbieters, über den Software für die Verwaltung von Geräteeinstellungen und Ressourcen bereitgestellt wird. Mit MDM können Schulen Geräte für die Nutzung durch Schüler einrichten, indem sie Apps, Bücher und andere Lerninhalte installieren, die von der Schule bereitgestellt werden. Die Schulverwaltung legt die Richtlinien für die Aktivierung oder Deaktivierung von Features auf dem iPad und Mac, in Apps und im Schulnetzwerk fest. MDM-Software ist in der Regel erforderlich, um schuleigene Geräte zu verwalten. In einem BYOD-Szenario ist sie optional.

Wenn das Gerät Ihres Schülers Eigentum der Schule ist, können die MDM-Einstellungen für iPad und Mac so konfiguriert werden, dass die Einstellungen nicht entfernt werden können. Das ist das Standardverfahren bei den meisten One-to-One-Implementierungen und Implementierungen mit geteilter Nutzung. Für Schulen, die das Feature „Geteiltes iPad“ nutzen, ist MDM erforderlich.

Wenn Schüler ihr eigenes Gerät mitbringen, müssen sie sich bei der Verwaltungssoftware der Schule anmelden. In diesem Fall können die MDM-Geräteeinstellungen von einem Schüler oder Elternteil jederzeit entfernt werden, da die Schule nicht Eigentümer des Geräts ist.

IT-Administratoren haben auf verwalteten Apple Geräten nur eingeschränkten Zugriff auf Schülerdaten und Standortinformationen. Mit MDM-Software können nicht alle Daten auf dem Gerät eines Schülers eingesehen werden. Die Software kann mit einem Gerät nur über Benachrichtigungen kommunizieren, die zum Konfigurieren von Einstellungen oder zum Installieren von Apps verwendet werden. Dies verhindert, dass Geräte der Schüler überwacht oder nachverfolgt werden. Wenn ein Gerät verloren geht oder gestohlen wird, kann ein IT-Administrator dieses Gerät mit dem Feature verwalteter Modus „Verloren“ ausfindig machen, jedoch nur, nachdem eine Nachricht an das Gerät gesendet und der Benutzer darüber informiert wurde, dass es verloren gegangen ist und auf seinen Standort zugegriffen wird. Wenn der Administrator den verwalteten Modus „Verloren“ deaktiviert, wird der Benutzer sowohl über eine Nachricht auf dem Sperrbildschirm als auch eine Benachrichtigung auf dem Homescreen informiert.

Apple School Manager und Schülerdaten

Apple School Manager, ist das IT-Verwaltungsportal von Apple, bei dem von Anfang an den Datenschutz der Schüler gedacht wurde. Beispielsweise importiert der Apple School Manager nur die Daten, die für die Einrichtung eines einfachen Accounts und Stundenplans erforderlich sind. Andere Schülerdaten, über die die Schule möglicherweise verfügt, werden nicht importiert. Ihre Schule kann den Apple School Manager verwenden, um verwaltete Apple IDs für Schüler, Lehrer und andere Mitarbeiter zu erstellen.

Konfigurieren von Geräten

Ihre Schule entscheidet, wie iPad und Mac Geräte konfiguriert werden, um die Anforderungen einer bestimmten Jahrgangsstufe oder eines bestimmten Lehrplans zu erfüllen. Die Einrichtung von Apps und Inhalten erfolgt, indem eine Datei an das Gerät gesendet wird, die ihm mitteilt, welche Einstellungen, Features und Apps verwendet werden sollen. Diese Datei, das Konfigurationsprofil, wird von der Schule verwaltet. Wenn die Schule MDM nicht verwendet, kann die Schulverwaltung Links zum Laden von Konfigurationsprofilen per E-Mail bereitstellen oder sie kann mit dem Apple Configurator, einem auf dem Mac verfügbaren Tool, manuell Profile auf Geräten installieren.

Bei One-to-One-Szenarien ist es verbreitet, dass Schulen MDM zum Einrichten und Verwalten von Geräten verwenden. Schüler erhalten in der Regel am ersten Schultag Geräte mit ihrer eigenen verwalteten Apple ID.
(Weitere Informationen zu verwalteten Apple IDs und MDM finden Sie auf Seite 1 im Abschnitt über Schüler-Accounts.)

Bei der Implementierung mit geteilter Nutzung können Geräte allgemein mit Standard-Apps und -Lernmaterialien eingerichtet werden. Eine sehr allgemeine Implementierung mit geteilter Nutzung erfordert möglicherweise nicht, dass ein Schüler sich mit einer Apple ID anmeldet. Mit der Software iOS 9 (oder neuer) ermöglicht das Feature „Geteiltes iPad“, dass das iPad für jeden Schüler personalisiert werden kann. Um auf diesen Mehrbenutzermodus zuzugreifen, verwendet Ihr Schüler eine verwaltete Apple ID, die von der Schule erstellt wurde. Mit ihr können Schüler ihre eigenen Arbeiten und Einstellungen speichern, und zwar jedes Mal, wenn sie ein iPad im Unterricht verwenden. Mit dem Feature „Geteiltes iPad“ werden die Daten der Schüler sicher auf dem Gerät und in iCloud gespeichert, sodass alle Schülerdaten geschützt sind.

Nicht verwaltete Geräte

Wenn Ihr Schüler ein eigenes iPad oder einen eigenen Mac in der Schule verwendet (BYOD), wird das Gerät nicht zwingend von der Schule verwaltet. An einigen Schulen ist es erforderlich, dass sich Schüler bei der von der Schule bereitgestellten Verwaltungssoftware anmelden, selbst wenn das Gerät ihr privates Eigentum ist. Schulen haben verschiedene Richtlinien. Fragen Sie daher Ihre Schulverwaltung, wie Geräte in Ihrem BYOD-Programm verwaltet werden.

Classroom App

Classroom ist eine iPad App von Apple, mit der Lehrer mit dem iPad das Lernen im Unterricht betreuen können. Mit der App können Lehrer bestimmte Apps auf allen iPads der Schüler im Unterricht starten, Websites teilen, Aktivitätsgruppen erstellen und die Displays der Schüler mit Bildschirmansicht einsehen. Lehrer können außerdem mithilfe von AirPlay und Apple TV das Display eines Schülers mit der restlichen Klasse teilen. Um Schülern konzentriertes Arbeiten zu ermöglichen, können Lehrer Geräte bis auf eine bestimmte App sperren oder alle Displays aller Geräte vorübergehend sperren.

Die Classroom App ist ein großartiges Tool für Lehrer, wurde aber auch entwickelt, um optimale Vorgehensweisen für Transparenz und Datenschutz der Schüler sicherzustellen. Das bedeutet, dass iPad Geräte von Schülern nur im Unterricht verwaltet werden. Der Lehrer kann die Geräte von Schülern nicht außerhalb des Unterrichts verwalten oder einsehen. Um Transparenz bei der Verwendung der Bildschirmansicht für das Display eines Schülers im Unterricht sicherzustellen, zeigt eine Benachrichtigung am oberen Bildschirmrand an, dass es eingesehen wird. Schulen können die Bildschirmansicht auch deaktivieren, wenn sie es vorziehen, dass Lehrer nicht die Displays der Schüler einsehen können.

Digitale Kompetenz

Technologie auf sichere und verantwortungsvolle Weise zu nutzen, nennt man auch digitale Kompetenz. Diese Praktiken umfassen Leitlinien für Internetsicherheit, Kommunikation, Cybermobbing, Informationskompetenz, kreatives Eigentum, Urheberrecht und vieles mehr. Da sich das Lernen in Schulen heute anders gestaltet als noch vor wenigen Jahren, ist es für die Schulen wichtig, diese Best Practices anzuwenden. Alle Schüler, Lehrer, Mitarbeiter und die Schulgemeinschaft sollten in diesen digitalen Kompetenzen geschult werden.

Es gibt viele Ressourcen, die Schüler dabei helfen, digitale Kompetenzen zu erwerben und auch Schulen und Lehrer dabei unterstützen. Common Sense Media stellt Materialien für Schulen und ihre Gemeinschaft zur Verfügung. Eltern und Schüler sollten auch die Technologierichtlinien ihrer Schule in Bezug auf akzeptable Nutzung, E-Mails, Speichern und Laden von Geräten, den Zugriff auf Inhalte und Apps und andere Themen lesen.

Ressourcen zu digitaler Kompetenz

Digitale Kompetenz auf iTunes: www.itunes.com/digitalcitizenship

Leitfaden für Datenschutz von Schülern des Future Privacy Forum: https://ferpasherpa.org/parents/a-parents-guide-to-student-data-privacy/

Common Sense Media

- Digitale Kompetenz: https://www.commonsensemedia.org/educators/digital-citizenship
- Leitfaden für Familien: https://www.commonsensemedia.org/guide/essentialbooks
- Leitfaden für Apps: https://www.commonsensemedia.org/guide/best-first-kids-apps

Ressourcen

Weitere Informationen darüber, wie Apple die Sicherheit und den Datenschutz von Schülern gewährleistet, finden Sie in untenstehenden Ressourcen. Falls Sie Fragen zum Datenschutz haben, können Sie uns auch direkt unter www.apple.com/de/privacy/contact kontaktieren.

- Apples Engagement für den Schutz Ihrer Daten: www.apple.com/de/privacy
- Überblick von Daten und Sicherheit für Schulen: http://images.apple.com/de/education/docs/Education_Privacy_Schools.pdf
- Hilfe zu Apple School Manager: help.apple.com/schoolmanager
- iCloud Sicherheit und Datenschutz: https://support.apple.com/de-de/HT202303
- Kindersicherung auf Apple Geräten: https://support.apple.com/de-de/HT201304
- iTunes U Sicherheit und Datenschutz: https://support.apple.com/de-de/HT204918