Nutzungsordnung der Stadt Rietberg
für die leihweise Überlassung
städtischer/schulgebundener mobiler Endgeräte
an Schülerinnen und Schüler
für den Einsatz zu unterrichtlichen Zwecken
an den Schulen der Stadt Rietberg
vom 7. Juni 2023

Mobile digitale Endgeräte, in diesem Fall iPads, dienen der Arbeit im Unterricht, an außerschulischen Lernorten, im Ganztag und zu Hause. Sie werden nach den Medienkonzepten der Schulen von den Lehrkräften im Unterricht als didaktische Hilfsmittel eingesetzt und von den Schülerinnen und Schülern als Lernwerkzeuge genutzt. Ihr Erfolg hängt von dem verantwortungsvollen Umgang jedes/jeder einzelnen damit ab.
Die Stadt Rietberg hat die Regio IT mit dem EDV-Support der städtischen Schulen beauftragt. Der Ausschuss für Schule und Kita der Stadt Rietberg hat im August 2022 beschlossen, alle Schülerinnen und Schüler schrittweise mit einem mobilen Endgerät leihweise auszustatten. Das mobile Endgerät wird der Schülerin oder dem Schüler, bei Minderjährigen nur mit schriftlicher Zustimmung der Erziehungsberechtigten/des Erziehungsberechtigten, zur Verfügung gestellt. Daher sollte die Nutzungsordnung von allen Beteiligten genau gelesen werden. Bei Unklarheiten sprechen Sie bitte mit der in der Schule verantwortlichen Person.

§ 1: Anwendungsbereich

Die Regelungen in dieser Nutzungsordnung sind auf

- die Ausleihe und Nutzung mobiler Endgeräte,
- die Nutzung des schulischen Netzwerks sowie des Internetzugangs und
- die Nutzung sonstiger in Zusammenhang damit stehender Dienste

durch Schülerinnen und Schüler anzuwenden.

§ 2: Ausstattung

Die Stadt Rietberg stellt die folgende Ausstattung zur Verfügung:

- Die Ausstattungsgegenstände sowie der ersichtliche Zustand werden in der **Anlage 2** aufgeführt.

Die Ausleihe beginnt mit der Ausgabe des mobilen Endgeräts zum Schuljahresbeginn und endet fünf Schultage vor dem letzten Schultag an der jeweiligen Schule.

Verlässt die Schülerin oder der Schüler vor dem Ende der Ausleihe die Schule, so endet die Zeit der Leihgabe mit Ablauf des letzten Tages der Schülerin oder des Schülers an dieser Schule.
Die Schülerin oder der Schüler hat das Endgerät mit Zubehör unverzüglich nach Ablauf der Leihdauer in ordnungsgemäßem Zustand an die Schule zurückzugeben.

§ 3: Nutzungsberechtigung für Leihgeräte

Die Schulleitungen entscheiden nach Maßgabe des Medienkonzepts der Schulen darüber, in welchem Rahmen die mobilen Endgeräte im Unterricht bzw. für Unterrichtszwecke (z.B. Vor- und Nachbereitung) eingesetzt werden.
Voraussetzung für die Ausleihe ist,

- dass die Schülerinnen und Schüler von der Schule/den Lehrkräften in den verantwortungsvollen Umgang mit den Endgeräten eingewiesen wurden und
- dass die Schülerin oder der Schüler (bei Minderjährigen auch die Erziehungsberechtigten) diese Nutzungsordnung in der jeweils geltenden Fassung schriftlich anerkannt haben.

Die Ausleihe erfolgt im Rahmen der vorhandenen Kapazitäten (insbesondere Verfügbarkeit der Leihgeräte) und der technischen Möglichkeiten durch eine von der Schulleitung bestimmte Person/Stelle.
Verstöße gegen die Nutzungsordnung können erzieherische Einwirkungen, wie z.B. den zeitweisen Entzug des mobilen Endgeräts, oder Ordnungsmaßnahmen zur Folge haben.
Bei Schadensfällen, Diebstahl oder Verlust des Geräts ist die Schulleitung unverzüglich zu informieren. Bei Ausscheiden aus der Schule ist das mobile Endgerät inklusive Zubehör der Schule zurückzugeben. Die Rückgabe der Endgeräte inklusive Zubehör erfolgt mittels **Anlage 2.**

§ 4: Kosten

Die Überlassung der schulischen mobilen Endgeräte erfolgt leihweise und ist für die Schülerinnen und Schüler kostenlos.

Die schulische Informationstechnologie, der Zugang zum schulischen Netzwerk und zum Internet sowie die weiteren damit in Zusammenhang stehenden sonstigen Dienste (z.B. Online-Lernplattformen) werden ebenfalls den Schülerinnen und Schülern unentgeltlich zur Verfügung gestellt.

§ 5: Sorgfaltspflichten

Schülerinnen und Schüler sind für das ihnen von der Schule leihweise überlassene mobile Endgerät einschließlich des Zubehörs (siehe **Anlage 2**) verantwortlich. Sie müssen damit sorgsam umgehen und es vor Bruch, Diebstahl, Verunreinigungen und Nässe schützen.

Das mobile Endgerät inklusive des Zubehörs muss im Unterricht einsatzbereit sein. Dies betrifft insbesondere den Ladezustand der Akkus. Die von der Schule bereitgestellten Anwendungen und Programme dürfen nicht gelöscht werden. In den Pausen bleibt das mobile Endgerät im verschlossenen Klassenzimmer. Bei der Bedienung des Geräts sind die Anweisungen der Lehrkraft zu befolgen. Störungen oder Schäden sind der Schule unverzüglich zu melden.

Die mobilen Endgeräte inklusive Zubehör sind nicht über die Stadt versichert. Der Abschluss einer Versicherung obliegt der Nutzerin bzw. dem Nutzer. Wer einen Schaden/Verlust/Diebstahl schuldhaft verursacht, hat diesen im Rahmen der gesetzlichen Bestimmungen zu ersetzen.

§ 6: Nutzungsbedingungen

- Die Schülerin/der Schüler ist für den sicheren und rechtmäßigen Einsatz des zur Verfügung gestellten mobilen Endgeräts verantwortlich, soweit sie/er hierauf Einfluss nehmen kann.
- Die Schülerin/der Schüler verpflichtet sich, sich an die geltenden Rechtsvorschriften – auch innerschulischer Art – zu halten. Dazu gehören insbesondere das Urheberrecht, der Jugend- und Datenschutz, das Strafrecht sowie die Schulordnung.
- Unabhängig von der gesetzlichen Zulässigkeit ist es bei der Nutzung des mobilen Endgeräts nicht gestattet, verfassungsfeindliche, rassistische, gewaltverherrlichende oder pornografische Inhalte willentlich oder wissentlich abzurufen, zu speichern oder zu verbreiten.
- Die Schülerin/der Schüler verpflichtet sich, zu jeder Zeit Auskunft über den Verbleib des mobilen Endgeräts geben zu können und dieses der Schule und dem Schulträger jederzeit vorzuführen. Sie/er trägt dafür Sorge, das Leihobjekt pfleglich zu behandeln.

- Besteht der Verdacht, dass das geliehene mobile Endgerät oder ein Computerprogramm/App von Schadsoftware befallen ist, muss dies unverzüglich der Schule/dem Schulträger gemeldet werden. Das mobile Endgerät darf im Falle des Verdachts auf Schadsoftwarebefall solange nicht genutzt werden, bis die Schule die Nutzung wieder freigibt.
- Sofern die Schulleitung es Schülerinnen und Schülern gestattet hat, das geliehene mobile Endgerät auch außerhalb der Schule zur Durchführung der Vor- und Nachbereitung des Unterrichts, für Projekttage, Praktika oder auf Klassenfahrten zu nutzen, ist diese Nutzungsordnung entsprechend anzuwenden.
- Da die Aufsicht von Lehrkräften bei der Vor- und Nachbereitung des Unterrichts außerhalb der Schule nicht wahrgenommen werden kann, sind die Erziehungsberechtigten in diesem Fall dafür verantwortlich, dass ihr noch nicht volljähriges Kind sich an die in dieser Nutzungsordnung enthaltenen Regeln hält.
- Eine Nutzung für private und andere nichtschulische Zwecke ist nicht zulässig.
- Die Überlassung des mobilen Endgeräts an andere Personen ist nicht zulässig.
- Eine kurzfristige Weitergabe an andere Schülerinnen und Schüler oder an Lehrkräfte ist erlaubt, soweit hierfür eine schulische Notwendigkeit besteht.
- Im öffentlichen Raum darf die Ausstattung nicht unbeaufsichtigt sein.

§ 7: Zugang zur Software des mobilen Endgeräts

In der Grundkonfiguration sind auf den Endgeräten folgende Nutzeraccounts eingerichtet:

- Es werden vom Schulträger verwaltete AppleIDs ohne Cloud-Funktionalität für die Nutzung der iPads zur Verfügung gestellt.
- Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, die nach der ersten Anmeldung individualisiert werden können.
- Die Passwörter sind getrennt vom mobilen Endgerät unter Verschluss aufzubewahren.
- Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein könnte, muss es sofort geändert werden.
- Das Passwort kann vom Nutzer/der Nutzerin und dem Schulträger zurückgesetzt werden.

§ 8: Grundkonfiguration zur Gerätesicherheit

- Im Übergabezustand sind die mobilen Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Schadsoftware vorkonfiguriert.
- Die Schule hat zur Filterung bestimmter illegaler, verfassungsfeindlicher, rassistischer, gewaltverherrlichender oder pornografischer Internetinhalte einen Contentfilter eingesetzt. Mittels dieses Contentfilters werden die Inhalte von Webseiten während des Browserbetriebs hinsichtlich einzelner Wörter, Phrasen, Bilder oder Links, die auf einen entsprechenden Inhalt hindeuten, automatisiert gefiltert. Auf dem mobilen Endgerät wird der Zugriff auf diese Inhalte zusätzlich über den von Apple zur Verfügung gestellten Inhaltsfilter eingeschränkt. Der Zugriff auf jugendgefährdende Inhalte kann dennoch nicht vollständig ausgeschlossen werden.
- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das mobile Endgerät regelmäßig mit dem Internet verbunden sein. Meldungen des Betriebssystems oder von installierter Software zur Installation von Updates müssen ausgeführt werden.
- Die Verbindung zum Internet ist innerhalb der Schule automatisch vorkonfiguriert und sollte außerhalb der Schule nur über vertrauenswürdige Netzwerke erfolgen, z.B. über das eigene WLAN zu Hause oder einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zur Verfügung stehenden Netzwerke (z.B. im Café), sollte das Gerät nicht damit verbunden werden.
- Im Unterricht muss die Schülerin/der Schüler alle Benachrichtigungen deaktivieren, um Störungen zu vermeiden.

§ 9: Datensicherheit (Speicherdienste)

- Daten dürfen nur auf den durch die Schule freigegebenen Diensten gespeichert werden (z.B. Logineo-Plattform).
- Daten werden standardmäßig lokal auf dem mobilen Endgerät gespeichert.
- Der Schulträger übernimmt keine Verantwortung für den Datenverlust, insbesondere auch nicht aufgrund von Gerätedefekten oder unsachgemäßer Handhabung.

§ 10: Technische Unterstützung

Die technische Unterstützung durch den Schulträger/die Schule umfasst insbesondere:

- die Grundkonfiguration der mobilen Endgeräte.
- Der Schulträger/die Schule behält sich vor, jederzeit zentral gesteuerte Updates der auf den mobilen Endgeräten vorhandenen Software vorzunehmen, etwa um sicherheitsrelevante Lücken zu schließen.
- Apps und sonstige Software dürfen nur nach Genehmigung durch die Schule installiert werden. Die Installation erfolgt dezentral vom Schulträger. Liegt eine Genehmigung vor, muss die Software über Sicherheitsupdates eigenverantwortlich auf dem aktuellen Stand gehalten werden.
- Das mobile Endgerät wird zentral mit Hilfe einer Software über eine Mobilgeräteverwaltung administriert. Mit Hilfe der Mobilgeräteverwaltung überwacht und verwaltet der Schulträger/die Schule die mobilen Endgeräte. Der Schulträger/die Schule behält sich vor, über die Mobilgeräteverwaltung mobile Endgeräte wie folgt zu administrieren: insbesondere
    - Entsperrcode zurücksetzen,
    - Gerät sperren (Sperrcode aktivieren),
    - Gerät auf Werkseinstellungen zurücksetzen.
- Voraussetzung für die Einrichtung des mobilen Endgeräts und die Mobilgeräteverwaltung durch den Schulträger/die Schule ist die Verarbeitung der personenbezogenen Daten der Schülerinnen und der Schüler.

§ 11: Zugangsdaten

Die Nutzung der mobilen Endgeräte erfolgt mittels personalisierter Nutzerkennung. Das personengebundene mobile Endgerät der Schule ist mit einem Code vor unberechtigten Zugriffen zu schützen.

Die Passwörter sind geheim zu halten. Sie dürfen nicht an andere Personen weitergegeben werden.

Das Arbeiten ist ausschließlich mit dem von der Schule zur Verfügung gestellten Benutzerkonto (Account) oder dem Gastzugang erlaubt.

Wer ein fremdes Passwort erfährt, ist verpflichtet, dies der zuständigen Lehrkraft mitzuteilen.

§ 12: Fotos, Videos und Audioaufnahmen

Fotos, Videos oder Audioaufnahmen dürfen nur für schulische Zwecke erstellt werden. Sie sind nach Aufforderung durch die Lehrkraft zu löschen.

Andere Personen dürfen nur dann auf Fotos oder Videos aufgenommen werden, wenn deren schriftliche Einwilligung vorliegt.

Unterrichtsmitschnitte sind nur dann gestattet, wenn die Lehrkraft einen entsprechenden Auftrag erteilt hat.

Die Weitergabe von Foto-, Video- oder Audioaufnahmen an Dritte, auf denen Personen zu sehen oder zu hören sind, oder deren Veröffentlichung im Internet ist verboten. Entsprechendes gilt für das Posten der Aufnahmen in sozialen Netzwerken.

§ 13: Datenschutz

Bei der Verwendung personifizierter Zugänge werden personenbezogene Daten der Nutzerinnen und Nutzer gespeichert, siehe **Anlage 3: Apple School Manager – Überblick Datenschutz und Privatsphäre.**

Von dem zentralen Mobilgerätemanagement werden bei der Nutzung eines Endgeräts nur folgende personenunabhängige Daten erhoben:

- Seriennummer des Geräts,
- MAC-Adresse des Geräts nutzende WLANs,
- Datum und Uhrzeit der Gerätenutzung des regelmäßigen Abgleichs mit dem MDM,
- Standortdaten des Geräts (nur bei Ortung über den verloren Modus),
- installierte Anwendungen.

Für eine vollständige Auflistung siehe **Anlage 4: Jamf School Manager – Referenz zu Mobilgerätebestand und Kriterien.**

Die Erhebung dieser Daten dient der Sicherstellung des ordnungsgemäßen Betriebs, der Fehlersuche und -Korrektur sowie der Optimierung der IT-Infrastruktur.

Es erfolgt keine Leistungs- oder Verhaltenskontrolle.

Eine personenunabhängige, nur gerätebestimmende Standortermittlung aufgrund der Seriennummer erfolgt grundsätzlich nur zur Ahndung von Verstößen gegen die Nutzungsordnung oder zur Unterstützung bei Diebstahl und grundsätzlich nur auf Weisung durch die Schulleitung und den/die Medienbeauftragte/n. Eine Zuordnung vom betroffenen Nutzer bzw. der betroffenen Nutzerin auf die entsprechende Seriennummer (oder umgekehrt) erfolgt nur durch die Schulleitung.

Fragen in Zusammenhang mit der Verarbeitung personenbezogener Daten der Schülerinnen und Schüler bei der Verwendung von mobilen Endgeräten für schulische Zwecke und dem Einsatz von Online-Lernplattformen sowie der Ausübung ihrer Rechte können an die/den für die betreffende Schule zuständigen behördlichen Datenschutzbeauftragte/n gerichtet werden.

§ 14: Datensicherheit

Für die Sicherung der mit dem mobilen Endgerät verarbeiteten Daten, wie beispielsweise Hausarbeiten, Facharbeiten und Referate, sind die Schülerinnen und Schüler selbst verantwortlich. Der Verlust von Daten entbindet sie nicht von ihren unterrichtlichen Pflichten.
Nicht von der Schule/dem Schulträger zur Verfügung gestellte Fremdgeräte (z.B. Peripheriegeräte wie externe Laufwerke, USB-Sticks, Scanner und Digitalkameras, Kopfhörer) dürfen nur mit Zustimmung der Lehrkraft angeschlossen werden.

§ 15: Nutzung des Internets

Der von der Schule eröffnete Zugang zum Internet darf nur für schulische Zwecke verwendet werden.
Schülerinnen und Schüler sind für von ihnen veröffentlichte Inhalte und Äußerungen innerhalb der gesetzlichen Grenzen verantwortlich.
Die gesetzlichen Bestimmungen insbesondere des Straf-, Urheber- und des Jugendschutzrechts sind bei der Nutzung zu beachten. Ebenfalls zu achten sind die Persönlichkeitsrechte anderer Menschen. Diskriminierungen, persönliche Angriffe, Beleidigungen und Verleumdungen sind deswegen untersagt.
Mit dem Auftrag der Schule unvereinbar ist es, kommerzielle, religiöse oder parteipolitische Werbung zu veröffentlichen.
Im Namen der Schule dürfen weder Vertragsverhältnisse eingegangen noch kostenpflichtige Dienste benutzt werden.

§ 16: Nutzung von Online-Lernplattformen

Die Entscheidung, welche Online-Lernplattform (E-Learning) an der Schule verwendet wird, trifft die Schulleitung (in Abstimmung mit dem Schulträger) aufgrund eines Vorschlags der Lehrerkonferenz.
Die Online-Lernplattform (E-Learning) darf nur für schulische Zwecke genutzt werden.

Bei der Einrichtung des personalisierten Benutzerkontos, der Festlegung der Zugriffsrechte, der Auswahl der Funktionalitäten und den Auswertungsmöglichkeiten dürfen nur die personenbezogenen Daten erhoben und verarbeitet werden, die für die Wahrnehmung der pädagogischen Aufgaben der Schule erforderlich sind.
Benutzerinnen und Benutzer der Plattform erhalten nur Zugang zu den Programmteilen, die für sie vorgesehen sind.
Die Aktivitäten der Schülerinnen und Schüler werden grundsätzlich nicht überwacht, es sei denn, die Plattform wird für pädagogische Aufgaben (z.B. organisierte Chats zu bestimmten Themen, Gruppenarbeiten) genutzt, die benotet werden.
Schulexterne erhalten nur Zugriff auf geschützte Bereiche der Plattform, sofern dies erforderlich ist, um die Funktion des Systems zu gewährleisten.
Die bei der Nutzung automatisch erfassten und gespeicherten Daten über den Nutzer bzw. die Nutzerin und seine bzw. ihre Aktivitäten (Log-Daten) werden nur für die Überwachung der Funktionsfähigkeit und Sicherheit des Systems sowie bei Anhaltspunkten für einen Missbrauch der Plattform benutzt.

§ 17: Aufsicht

Zur Erfüllung ihrer gesetzlichen Aufsichtspflicht ist die Schule sowie das ggf. für das IT-System der Schule zuständige Personal des Schulträgers oder des von ihm bestellten Dienstleisters Regio IT berechtigt, die auf der schulischen Hardware gespeicherten Daten und die mit der schulischen Software und Informationstechnologie verarbeiteten Daten jederzeit zu speichern und zu kontrollieren (z.B. Nutzung und Installation von Anwendungen, durchgeführte Updates, Systemabstürze, An- und Abmeldungen).
Die Schulleitung und das für das IT-System der Schule zuständige Personal kann darüber hinaus bei Verdacht Einsicht in die Protokolldateien des Betriebssystems und des Internetbrowsers nehmen. Dies gilt insbesondere bei einem Verdacht von Missbrauch oder bei verdachtsunabhängigen Stichproben.

Stadt Rietberg
Der Bürgermeister

Anlage 1: Anerkennung der Nutzungsordnung der Stadt Rietberg für die leihweise Überlassung städtischer / schulgebundener mobiler Endgeräte an Schülerinnen und Schüler für den Einsatz zu unterrichtlichen Zwecken an den Schulen der Stadt Rietberg in der aktuell gültigen Fassung.

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsordnung vorzunehmen.

_____

Name, Vorname der Schülerin oder des Schülers

_____

Name, Vorname der Erziehungsberechtigten oder des Erziehungsberechtigen

_____

Name der Schule

_____

Datum und Unterschrift der Schülerin oder des Schülers und der Erziehungsberechtigten

_____

Datum und Unterschrift der Schulleitung in Vertretung des Schulträgers

Anlage 2: Übergabe/Rückgabe der Ausstattung

Ausgabe durch _____, _____, _____
Name *Vorname* *Funktion*

Name der Schule _____ (Schulstempel).

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung:

    _____
  - Seriennummer:

    _____

- **Zubehör**
  - Netzteil
  - Pencil
  - Schutzhülle
  - Weiteres Zubehör individuell ergänzen
  -

- **Zugangsdaten**
  - individuelle Angaben ergänzen
  -

- **Zustand**

  [ ] neu

  [ ] Vorschäden

  Beschreibung (ggf. Foto bzw. Zeichnung hinzufügen)

  _____

  _____

  _____

_____

Geräte Annahme: Datum und Unterschrift Personensorgeberechtigte/n

_____

Geräte Rückgabe: Datum und Unterschrift Personensorgeberechtigte/n

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 hinzufügt. 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, Kalendereereignisse 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

Referenz zu Mobilgerätebestand und Kriterien

Bestandsattribut/Kriterium	Hinweise
Name des Mobilgeräts	Diese Information kann nur für betreute Geräte bearbeitet werden, wenn die Option Name des Mobilgeräts aktiviert ist. Bei Auswahl der Option „Name des Mobilgeräts erzwingen“ wird der Name des Mobilgeräts von Jamf Pro auf eine von zwei Arten durchgesetzt: • Wenn der durchgesetzte Gerätename von dem Gerätenamen abweicht, der im aktuellen Bestandsdatensatz des Geräts hinterlegt ist, wird von Jamf Pro ein MDM-Befehl zum Umbenennen des Geräts gesendet. • Wird der in Jamf Pro festgelegte Gerätename vom Endbenutzer geändert, wird von Jamf Pro bei der nächsten Übermittlung von Bestandsinformationen ein MDM-Befehl zum Umbenennen des Geräts gesendet.
Jamf Pro Mobilgeräte-ID (Kriterium „Geräte-ID“)	
Asset-Tag	
Standort	
Letzte Bestandsaktualisierung	
iOS Version	Für Apple TV Geräte mit tvOS bis Version 10.2 entspricht die iOS Version der Build-Version des Betriebssystems, auf der die Apple TV Software basiert. Die Version der installierten Apple TV Software wird nicht erfasst. Bei Apple TV Geräten mit tvOS 10.2 oder neuer wird die installierte tvOS Version angezeigt.
iOS Build	
Geräte-ID für Softwareupdates	
IP-Adresse	
Verwaltet	
Betreut	
Geteiltes iPad	Zeigt an, ob Geteiltes iPad für betreute iPad Geräte unter iOS 9.3 oder neuer aktiviert wurde
Diagnose- und Nutzungsberichte	Nur Geteiltes iPad
App-Analysen	Nur Geteiltes iPad

Bestandsattribut/Kriterium	Hinweise
Anzahl der Benutzer	Zeigt die Anzahl der Benutzeraccounts, die auf dem Gerät zwischengespeichert sind Nur Geteiltes iPad
Größe des Speicherkontingents (Kriterium „Quota Size [Kontingentgröße]“)	Nur Geteiltes iPad
Nur temporäre Sitzung	Nur Geteiltes iPad
Zeitüberschreitung für temporäre Sitzung	
Zeitüberschreitung für Benutzersitzung	
Maximale Benutzeranzahl für geteilte iPad Geräte gespeichert	Gibt die maximal zulässige Anzahl von Benutzeraccounts an, die für Geteiltes iPad gespeichert werden können.
Art der Geräteeigentümerschaft	
Registrierungsmethode	
Last Enrollment	
Ablaufdatum des MDM-Profils	
Geräte Lokalisierungs Dienst aktiviert	Gibt an, ob auf dem Mobilgerät die Funktion „Mein iPhone/iPad suchen“ aktiviert ist.
Nicht stören	
iCloud Sicherung (Kriterien für letztes Backup)	
Letzte iCloud Sicherung	
Bluetooth Low Energy-Unterstützung	Um die Unterstützung für Bluetooth Low Energy ermitteln zu können, muss auf dem Mobilgerät Jamf Self Service für iOS installiert sein. Wenn Self Service auf dem Gerät zuvor noch nicht gestartet wurde, wird der Wert „Nicht fähig/unbekannt“ zurückgegeben.
Ortungsdienste für Self Service	Gibt an, ob für die Jamf Self Service App auf dem Mobilgerät die Ortungs-Dienste aktiviert wurden. Um herauszufinden, ob die Ortungs-Dienste für Self Service aktiviert wurden, muss auf dem Gerät Jamf Self Service für iOS installiert sein. Wenn Self Service auf dem Gerät bisher überhaupt nicht oder seit dem Hinzufügen des anfänglichen iBeacon Bereichs zu Jamf Pro nicht gestartet wurde, wird der Wert „Nicht aktiviert/unbekannt“ zurückgegeben.
Beim App Store angemeldet	
Exchange Geräte-ID	
Tethering-Status	
Zeitzone	
AirPlay Passwort	Nur Apple TV Geräte