Allgemeine Überlegungen

Adressaten

Diese Empfehlungen richten sich an Personen, welche iPads als dienstliche Endgeräte für Lehrkräfte an Schulen in Niedersachsen einrichten und verwalten: Mitarbeiter aus der IT Abteilung des Schulträgers, Mitarbeiter eines vom Schulträger beauftragten Dienstleisters und in der Schule mit Administrationsaufgaben betraute Lehrkräfte.

Zielsetzung

Mit diesen Empfehlungen soll den Personen, welche iPads als dienstliche Endgeräte für die Verarbeitung von personenbezogenen Daten in der Schule einrichten und verwalten, eine Orientierung gegeben werden, wie sie die von ihnen betreuten Geräte mit Bezug auf die Sicherheit und den Schutz der auf den Geräten verarbeiten personenbezogenen Daten über das von ihnen genutzte Mobile Device Management (MDM) konfigurieren können.

Die hier abgegebenen Empfehlungen sind, genau dieses - Empfehlungen. Wo sinnvoll, sind die einzelnen Einschränkungen bzw. Einstellungen mit Erläuterungen versehen. Diese sollen helfen, zu entscheiden, ob und wie Einschränkungen in bestimmten Bereichen gesetzt werden. Es muss letztlich jede Institution für sich entscheiden, wie eng man sich an diese Empfehlungen hält und wo man davon abweichen möchte. Dafür muss abgewogen werden zwischen den geplanten Nutzungszwecken und der damit einhergehenden Verarbeitung von personenbezogenen Daten sowie den sich daraus ergebenden Schutzbedarfen.

Rechtlicher Hintergrund

Im Rahmen der „Richtlinie über die Gewährung von Zuwendungen zur Förderung des Programms 'Leihgeräte für Lehrkräfte' des Bundes und der Länder und Richtlinie über die Gewährung von Zuwendungen zur Verbesserung der IT-Infrastruktur und der IT-Ausstattung in Schulen“ stellen viele Schulträger den Lehrkräften ihrer Schulen iPads als Leihgeräte zur Verfügung. Anders als z.B. in Nordrhein-Westfalen haben diese Geräte in Niedersachsen lediglich den Status eines privaten Endgerätes, für das die entsprechenden Regelungen des Bezugserlasses „Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen (IT-Systemen) von Lehrkräften“ gilt.

Die regionalen Landesämter für Schule und Bildung stellen umfangreiche Informationen zur Auslegung des Erlasses bereit. Die Verarbeitung personenbezogener Daten auf technisch nicht intervenierbaren Systemen wie iOS, iPadOS, ChromeOS oder Android ist auf privaten Endgeräten oder solchen, die privaten Endgeräten gleichgestellt sind, untersagt. Es ist davon auszugehen, das dienstliche Daten auf iPads, die im Kontext der Förderrichtlinie beschafft wurde, generell nicht lokal gespeichert dürfen.

Viele Träger möchten Ihren Lehrkräften allerdings Endgeräte zur Verfügung stellen, mit denen die Verarbeitung dienstlicher Daten möglich ist. In vielen Fällen sind das iPads. Diese iPads für Lehrkräfte müssen dafür die technischen Vorgaben eines dienstlichen Gerätes erfüllen. Das bedeutet die Fernkonfiguration über ein MDM mit entsprechend datenschutzfreundlichen Einstellungen. Eine **Verpflichtung der Träger**, eine solche Konfiguration und zusätzliche Beschaffung von iPads vorzunehmen **besteht nicht**. Es handelt sich um eine freiwillige Leistung.

Bei der Einrichtung und Verwaltung von dienstlich genutzten iPads stehen zwei Bereiche im Fokus, Datenschutz und Datensicherheit. Es geht einmal

- um die durch die Lehrkräfte verarbeiteten personenbezogenen Daten aus der Schule und dann auch
- um die der Lehrkräfte als Nutzer selbst.

Um die Vorgaben zur Verarbeitung von personenbezogenen Daten aus der Schule gemäß dem NSchG §31 sowie allgemeinen datenschutzrechtlichen Grundsätzen einzuhalten, muss sichergestellt werden, dass

- die Verarbeitung sicher ist und
- die verarbeiteten Daten jederzeit verfügbar sind.

Trotz Übernahme der Konfiguration durch den Träger bleibt die Schule verantwortliche Stelle im Sinne der DS-GVO.

Die Sicherheit der Verarbeitung wird gewährleistet durch a) den Zugriffsschutz und b) die Verschlüsselung der Daten auf dem iPad. Während die Verschlüsselung sämtlicher Daten auf dem Gerät im Standard aktiviert ist, muss der Zugriffsschutz durch die Verwaltung vorgegeben oder vom Nutzer selbst aktiviert werden. Die Verfügbarkeit wird zum einen durch die Sicherheit der Verarbeitung gewährleistet und zum anderen durch eine regelmäßige Sicherung der verarbeiteten Daten außerhalb des Gerätes.

Vorüberlegungen

Ein Gerät - zwei Nutzungszwecke

Die dienstlichen iPads sind gemäß der Richtlinie zur Unterstützung von Lehrkräften bei der rechtssicheren Verarbeitung von personenbezogenen Daten gedacht. Damit ist jedoch nicht nur die Verarbeitung von personenbezogenen Daten im Rahmen der pädagogischen Dokumentation und der schulinternen Verwaltung gemeint. An vielen Schulen sind iPads bereits für pädagogische Zwecke im Einsatz. iPads wurden dort als Dienstgeräte für die Lehrkräfte ausgewählt, um diese iPads auch im Unterricht für pädagogische Zwecke einzusetzen, etwa zur Kontrolle und Steuerung der Schüler iPads über Apple Classroom oder zum Verteilen von Materialien via AirDrop. Bei der Einrichtung und Verwaltung der Geräte sollte dieser Umstand der dualen Nutzung berücksichtigt werden.

Angemessenheit der Maßnahmen

Über Einschränkungen ist es möglich, viele Funktionen von iPads und über iOS und die iCloud mit dem Gerät verbundene Dienste komplett zu unterbinden. Je stärker über das MDM in diese Funktionen eingegriffen wird, umso mehr schränkt dies die Nutzbarkeit des Gerätes ein. Aus diesem Grund ist bei der Einrichtung und Verwaltung der dienstlichen iPads eine Abwägung zu treffen zwischen den für eine Verarbeitung von personenbezogenen Daten erforderlichen Schutzmaßnahmen und den für eine unterrichtliche Nutzung sinnvollen Freiheiten. Dabei ist zu berücksichtigen, dass die Schutzbedarfe auch von den Arten von personenbezogenen Daten, welche eine Lehrkraft verarbeitet, abhängen und zu treffende Schutzmaßnahmen von daher bezüglich der geplanten Nutzung differenziert zu betrachten sind.

Sollen auf einem dienstlichen iPad lediglich Noten verarbeitet werden, Bemerkungen über Schüler, Absenzen, Auswertungen von Klassenarbeiten, von Schülern erstellte Artefakte zur Bewertung und Fotos von Schülern, wie dieses bei einer Fachlehrkraft der Fall ist, dann ist der Schutzbedarf deutlich geringer als bei einer Lehrkraft mit Klassenleitungsfunktion, die auf ihrem iPad die kompletten Zeugnisnoten ihrer Schüler verarbeitet, Bemerkungen zum Sozialverhalten sammelt, Protokolle von Klassenkonferenzen und Beratungsgesprächen anfertigt und Elternanschreiben bezüglich Ordnungsmaßnahmen darauf erstellt. Die Erfordernis für qualifizierte Einwilligungserklärungen, z.B. für die Nutzung von Schüler:innenfotos zu pädagogischen Zwecken bleibt unberührt. Noch höher ist der Schutzbedarf, wenn eine Person in einer Schulleitungsfunktion ist und über das Gerät Zugriff auf in der Schulverwaltung gespeicherte personenbezogene Daten hat, darauf dienstliche

Beurteilungen erstellt und Informationen über Lehrkräfte speichert oder bei einer Förderschullehrkraft, welche auf dem Gerät personenbezogene Daten im Zusammenhang mit der Erstellung von Fördergutachten verarbeitet.

Es wird sicher Schulen geben, an welchen dienstliche iPads für alle die oben beschrieben Zwecke eingesetzt werden sollen. Genauso werden andere Schulen aufgrund ihrer technischen Ausstattung in der Lage sein, iPads nur für einen Teil der beschriebenen Zwecke einzusetzen und für die anderen Zwecke auf alternative Geräte der Schule auszuweichen.

Nur ein Profil in Niedersachsen

Konfiguration und Verwaltung der dienstlichen iPads sollten sich immer am geplanten Nutzungszweck der Geräte orientieren. Aufgrund der Rechtslage in Niedersachsen ist grundsätzlich von einem hohen bis sehr hohen Schutzbedarf, in der Regel den Schutzstufen C und D, ggf. auch E auszugehen.

Technische und organisatorische Maßnahmen balancieren

Einen einhundertprozentigen technischen Schutz kann es nie geben bei der Verarbeitung von personenbezogenen Daten. Dieses sollte bei der Auswahl der Maßnahmen zum Schutz und zur Sicherheit der Verarbeitung von personenbezogenen Daten auf den dienstlichen iPads berücksichtigt werden. Es ist deshalb sinnvoll, technische Maßnahmen in Form der Einschränkung von Funktionen über das MDM mit organisatorischen Maßnahmen in Form von Verhaltensregeln (als Nutzungsvereinbarung und/ oder Dienstanweisung) und Schulungen der Nutzer zu kombinieren, um größtmöglichen Schutz und Sicherheit bei der Verarbeitung zu erreichen, ohne dabei das Gerät durch technische Einschränkungen in seinen Funktionen zu stark zu beschränken. Dabei kann der Anteil der technischen und organisatorischen Maßnahmen von Schutzstufe zu Schutzstufe unterschiedlich ausfallen.

Adaptabilität von Maßnahmen

Nichts ist in Stein gemeißelt. Das gilt für diese Empfehlungen und es gilt für die technischen und organisatorischen Maßnahmen, auf die man sich letztendlich geeinigt hat und die man dann in die Praxis umsetzt. Schulträger und Schulen müssen bereit sein, diese Maßnahmen nachzujustieren, wenn sich zeigt, dass sie zu rigide sind, über das Ziel hinausschießen, in der Schule nicht alltagstauglich sind oder auch zu lax in einigen Bereichen. Auch wenn die Empfehlungen mit Blick auf Schule und den Alltag in Schule entwickelt wurden, so schauen sie wie vergleichbare Empfehlungen für die Nutzung von iOS Geräten in Wirtschaftsbetrieben und Behörden zuallererst auf die Sicherheit und den Schutz der verarbeiteten Daten. Sie gehen von Bedrohungsszenarien aus, die vielfach übertrieben scheinen, aber die Geräte absichern sollen für den Fall, dass doch etwas passiert, gemessen am Schutzbedarf der darauf verarbeiteten personenbezogenen Daten. Niemand käme auf die Idee, auf die Ausstattung von Autos mit Airbags und Sicherheitsgurten zu verzichten, weil Unfälle insgesamt doch recht selten sind.

Gerade das Anpassen von Einschränkungen in Profilen eines MDM ist wenig aufwändig. Haken werden gesetzt oder entfernt. Es sind Kleinigkeiten, doch sie können enorme Unterschiede machen. Deshalb sollte es nach einer verabredeten Zeit eine Evaluation geben, in welcher die Alltagserfahrungen der Lehrkräfte bei der Arbeit mit den verwalteten iPads erhoben werden, um daraus resultierend die Maßnahmen nachzujustieren.

Verarbeitung und Speicherung - auf dem Gerät & online

In Niedersachsen schließt die Verarbeitung von personenbezogenen Daten aus der Schule auf einem dienstlichen Endgerät auch die Speicherung auf dem Endgerät selbst mit ein. Diesem muss bei der Einrichtung und Verwaltung dieser Geräte Rechnung getragen werden. Entsprechend müssen getroffene Schutzmaßnahmen

die Verarbeitung und Speicherung auf dem Gerät selbst berücksichtigen wie auch die Verarbeitung von Daten, welche nicht auf dem Gerät selbst gespeichert werden. Letzteres meint die Verarbeitung in Online Plattformen, auf die entweder über einen Browser zugegriffen wird oder über ein App, welches keine lokale Datenspeicherung vorsieht.

Der Speicherung und Verarbeitung in einer abgesicherten Onlineumgebung, die den datenschutzrechtlichen Voraussetzung durch die DS-GVO gerecht wird, ist immer der Vorzug zu geben, insbesondere bei der Verarbeitung von Daten mit hohem und sehr hohem Schutzbedarf.

Risikoszenarien

Bei der Nutzung von dienstlichen iPads muss von mehreren Risikoszenarien ausgegangen werden.

Unbefugter Zugriff auf Daten

Nicht berechtigte Personen erlangen Zugriff auf personenbezogene Daten, welche auf oder über das dienstliche iPad verarbeitet werden. Dieses kann erfolgen, wenn der Zugriff auf das Gerät nicht gesichert ist oder es gelingt, den bestehenden Zugriffsschutz zu überwinden. In Folge können sie

- unbefugt Kenntnis erhalten von diesen Daten,
- Daten stehlen,
- Daten verändern,
- Daten löschen.

Unbefugte Übermittlung von Daten

Eine unbefugte Übermittlung findet statt, wenn auf oder über das Dienstgerät verarbeitete und gespeicherte personenbezogene Daten an Personen oder Dienste übermittelt werden, welche keine Berechtigung dafür besitzen. Dazu gehören:

- die Speicherung von Daten in Clouds, mit denen die Schule keinen Vertrag zur Auftragsverarbeitung abgeschlossen hat,
- die Speicherung in Clouds, deren Nutzung als nicht DS-GVO konform eingestuft wird,
- das Auslesen von Daten vom Gerät durch unbefugte Dritte,
- die Übermittlung von Daten an nicht berechtigte Dienste oder Personen durch Nutzerfehler/ Fehlbedienung

Verlust von Daten

Zu einem Verlust von Daten kann es durch verschiedene Szenarien kommen. Ein Verlust kann entstehen durch den Verlust des Gerätes selbst durch Diebstahl oder Fahrlässigkeit des Benutzers, sofern die darauf gespeicherten Daten nicht außerhalb des Gerätes gesichert werden,

- die Zerstörung des Gerätes,
- eine Fehlbedienung des Benutzers,
- unbefugten Zugriff durch Dritte auf
    - das Gerät selbst, wo sie gezielt Daten löschen oder das Gerät komplett zurücksetzen,
    - das Apple Konto des Gerätebenutzers, um es aus der Ferne zurückzusetzen

Nutzung von iCloud

iCloud ist ein für Schulen attraktives Angebot. Jeder managed Apple ID stehen 200 GB Online Speicher zur Verfügung, die über digitale Endgeräte und den Browser zugänglich sind. Für Nutzer von managed Apple IDs und privaten Apple IDs stellt iCloud neben dem Online Speicher eine Reihe von weiteren Funktionalitäten für angebundene Endgeräte zur Verfügung. Mit der Anmeldung an einem iOS oder mac OS Gerät wird dieses mit den Diensten der iCloud verbunden. Die auf iPads vorinstallierten System-Apps, die Apple als built-in Apps bezeichnet, synchronisieren ihre Inhalte in der Standardeinstellung automatisch in die iCloud, um sie dem Benutzer auf anderen von ihm genutzten Apple Geräten zur Verfügung zu stellen. Dieses ermöglicht auch die Continuity Funktion, über welche mittels Handoff die Arbeit in einem App wie Notes von einem Apple Gerät, etwa einem iPad, auf einem anderen, z.B. einem Mac, lückenlos fortgesetzt werden kann. Auch die Apple eigenen Apps Pages, Numbers und Keynote, sowie zahlreiche Apps von Drittanbietern unterstützen diese Funktionen.

iCloud ist auch Voraussetzung für die gemeinsame Arbeit verschiedener Nutzer an einem geteilten Dokument (engl. collaboration). Dabei hält iCloud die Eingaben der verschiedenen Mitarbeiter und den gemeinsamen Bearbeitungsstand für alle Mitarbeitenden synchron.

Über iCloud können auch die auf einem Endgerät im Schlüsselbund hinterlegten Nutzerdaten (engl. credentials) für verschiedene Websites, Apps, Wifi-Netzwerke gesichert und mit anderen Geräten des Nutzers synchron gehalten werden. Apple sichert die Übermittlung und Speicherung von Daten in iCloud im Minimum durch eine starke 128-bit AES Verschlüsselung. Die Schlüssel speichert Apple in gesicherten Datenzentren und sichert zu, diese Schlüssel niemals an Dritte weiterzugeben. Passwörter und Anmeldedaten der schulischen Nutzer werden nach Apples Angaben so gespeichert, dass selbst der Anbieter sie nicht lesen kann. Viele der Funktionen von iCloud wurden speziell mit Blick auf private Nutzer entwickelt. Sie können in Schule durchaus einen Nutzen haben, bringen jedoch mit Blick auf die Daten, welche auf dienstlichen iPads verarbeitet werden, auch datenschutzrechtliche Risiken mit sich.

Risiken

Für eine Speicherung, Backup und Synchronisation von auf dienstlichen iPads verarbeiteten personenbezogenen Daten sollte iCloud nicht genutzt werden, da aufgrund der aktuellen US amerikanischen Rechtslage nicht auszuschließen ist, dass US Ermittlungsbehörden Zugriff auf diese Daten erhalten. Zwar sichert Apple zu, die Schlüssel, mit welchen diese Daten verschlüsselt gespeichert werden, nicht an Dritte weiterzugeben, doch dieses schließt eine Übermittlung der Inhalte selbst nicht aus, nachdem Apple sie für US Ermittlungsbehörden entschlüsselt hat. Dass Apple Ermittlungsersuchen dieser Art nachkommt, ist aus verschiedenen Fällen der Vergangenheit belegt.

Steuerungsmöglichkeiten

Es gibt zwei Orte, an denen der Zugriff auf iCloud gesteuert werden kann. Über das MDM kann ein Administrator Funktionen der iCloud sowohl für verwaltete als auch nicht verwaltete Apps aktivieren und deaktivieren. Am iPad angemeldete Benutzer können iCloud Funktionen für verwaltete Apps, eigenständig abschalten, solange sie nicht über das MDM deaktiviert wurden. Außerdem können sie diese Funktionen für von ihnen installierte, nicht verwaltete Apps steuern.

Über das MDM ist es möglich,

- die folgenden Funktionen von iCloud für verwaltete und nicht verwaltete Apps zu aktivieren/ deaktivieren
  - „Sichern in iCloud erlauben“
  - „iCloud Dokumente und Daten erlauben“ (erforderlich für Continuity)

    - „iCloud Schlüsselbund erlauben“
    - „iCloud Fotomediathek erlauben“
    - „Synchronisieren verwalteter Apps mit iCloud erlauben“
    - „Fotostream erlauben“
    - „Gemeinsamen Fotostream erlauben“
- durch Deaktivierung von “Änderungen der Accounteinstellungen” die Anmeldung von Nutzern am iPad zu verhindern, wodurch die iCloud deaktiviert bleibt.

Über das MDM ist es nicht möglich,

- die Funktionen von iCloud für System-Apps zu aktivieren/ deaktivieren, wenn iCloud auf dem Gerät aktiv ist.

Über das iPad kann

- eine managed Apple ID die iCloud gezielt für alle System-Apps aktivieren/ deaktivieren,
- eine private Apple ID die iCloud gezielt für alle manuell installierten Apps sowie die System-Apps aktivieren/ deaktivieren,
- eine private Apple ID iCloud Drive aktivieren/ deaktivieren,

sofern iCloud auf dem Gerät durch das MDM zugelassen ist.

Maßnahmen

Verzicht auf Apple IDs

Werden die dienstlichen iPads komplett ohne Apple IDs genutzt, das meint sowohl ohne managed Apple IDs als auch ohne private Apple IDs, dann sind auf dem iPad keine iCloud Funktionen verfügbar. Es können keine personenbezogenen Daten vom dienstlichen iPad in die iCloud abfließen, auch nicht durch Bedienfehler des Benutzers.

Um die Anmeldung am dienstlichen iPad auszuschließen, wird die Einschränkung „Ändern der Accounteinstellungen (E-Mail. Kontakte, Kalender, iCloud und iTunes Store)“ genutzt. Mit dieser Einschränkung verlieren Nutzer auch die Möglichkeit, eigene Apps zu installieren. Funktionen für den Unterricht, welche eine Verbindung zu Apple Diensten voraussetzen, können nicht genutzt werden.

Bei Nutzung von Apple IDs

Benutzeranmeldung am Gerät

Bei einer Nutzung der dienstlichen iPads mit managed wie auch privaten Apple IDs, wird die iCloud durch die entsprechenden Einschränkungen im MDM für alle verwalteten Apps komplett deaktiviert. Es geht dabei sowohl um den Schutz der auf dem dienstlichen iPad verarbeiteten personenbezogenen Daten wie auch die Daten des Nutzers selbst. Da diese Einschränkungen nicht die System-Apps einschließen, müssen die Lehrkräfte über eine Dienstanweisung angewiesen werden, die iCloud für alle System-Apps manuell zu deaktivieren.

Eingeschränkter Schutz

Soll die iCloud für pädagogische Zwecke genutzt werden, darf die Funktion „iCloud Dokumente und Daten erlauben“ nicht deaktiviert sein. Lehrkräfte müssen dann angewiesen werden, iCloud manuell für alle Apps (einschließlich System-Apps) zu deaktivieren, mit denen personenbezogene Daten, die zur pädagogischen

Dokumentation und schulinternen Verwaltung gehören, verarbeitet werden. iCloud darf nur bei Apps aktiv bleiben, welche für pädagogische Zwecke benötigt werden.

Nutzeranmeldung am App Store

Ist am Gerät noch keine Apple ID angemeldet und Nutzer melden sich mit einer privaten Apple ID am App Store an, so wird iCloud dabei nicht automatisch mit aktiviert. Es besteht die Möglichkeit, iCloud über einen separaten Dialog zu aktivieren. Solange dieses unterbleibt, sind auf dem Gerät keine iCloud Funktionen verfügbar, weder für die über das MDM installierten Apps, noch für die System-Apps. Nutzer haben die Möglichkeit, eigene Apps zu installieren und zu nutzen, ohne dass diese auf iCloud zugreifen können. Um diese Maßnahme umzusetzen, braucht es eine entsprechende Nutzungsvereinbarung oder Dienstanweisung.

Apps

Mit Blick auf in einem MDM verwaltete dienstliche iPads kann man drei Gruppen von Apps unterscheiden. Über Einschränkungen können die verschiedenen Gruppen angesprochen und in ihren Funktionen gesteuert werden. So ist es unter anderem auch möglich, die Daten von verwalteten und nicht verwalteten Apps von einander getrennt zu halten.

System-Apps

Diese Apps sind auf jedem iOS Gerät im Auslieferungszustand vorhanden. Sie unterscheiden sich von den anderen beiden Gruppen durch höhere Berechtigungen. So zählen sie nicht zu den verwalteten Apps und können dadurch im MDM nicht mit den gleichen Einschränkungen gesteuert werden wie verwaltete Apps. Mit Blick auf iCloud gelten diese Apps als nicht verwaltet und iCloud ist für standardmäßig aktiviert.

Verwaltete Apps (managed Apps)

Diese Apps werden durch die Institution im VPP (Volume Purchase Program) gekauft und über das MDM Geräten oder Nutzern zugewiesen. Bei ihnen greifen alle Einschränkungen des MDM, auch wenn diese nicht speziell als für verwaltete Apps gekennzeichnet sind. Für verwaltete Apps können keine in App Käufe getätigt werden.

Nicht verwaltete Apps (unmanaged Apps)

Von Nutzern einer privaten Apple ID auf einem verwalteten iPad installierte Apps werden als nicht verwaltete Apps bezeichnet. In App Käufe sind hier möglich. Sie unterliegen den Einschränkungen, welche als für verwaltete Apps gekennzeichnet sind, nicht. Diese Einschränkungen können jedoch indirekt auf sie wirken.

Nutzung von Apple IDs

Die Nutzung von managed Apple IDs und/ oder privaten Apple IDs auf einem dienstlichen iPad muss unter verschiedenen Gesichtspunkten betrachtet werden.

Erfordernis

- Um ein Dienst iPad zu verwalten, braucht es weder eine managed Apple ID noch eine private Apple ID.
    - Moderne MDM können iPads als Geräte verwalten und diesen über Profile Apps und Einschränkungen zuweisen.

    - Von Nachteil ist dabei, dass über den VPP Store keine in App Käufe getätigt werden können. Apps, die es nicht als Paket gibt, in denen alle in App Käufe bereits enthalten sind, können nur in der oft kostenlosen Basisversion genutzt werden.
- Einige Funktionen, die von iOS bereitgestellt werden, benötigen eine Apple ID.
    - Mit Apple Classroom haben Lehrkräfte die Möglichkeit, die iPads der Schüler zu kontrollieren. So können sie beispielsweise den Bildschirm einsehen und iPads in einen Single App Modus versetzen.
        - Werden die Klassen in Apple Classroom über Apple School Manager (ASM) verwaltet, erfordert Apple Classroom zwingend die Nutzung von managed Apple IDs, sowohl bei Lehrkräften wie auch Schülern.
        - Alternativ können die Klassen über das MDM verwaltet werden. Managed Apple IDs sind dann optional. Sind Lehrer mit einer managed Apple ID am Gerät angemeldet, können sie auch die Passwörter von Schülern zurücksetzen, die auf shared iPads angemeldet sind.
        - Alternativ kann Apple Classroom genutzt werden, ohne dass die Klassen über ASM oder das MDM verwaltet werden. Dann dürfen auf den Geräten keine managed Apple IDs angemeldet sein.
    - Apple Schoolwork stellt Funktionen für den Unterricht bereit, mit welchen Lehrkräfte Schülern Aufgaben geben und ihre Fortschritte bei der Bearbeitung dieser Aufgaben einsehen können.
        - Zur Nutzung werden bei Schülern und Lehrkräften managed Apple IDs benötigt, die über den ASM der Schule verwaltet und Klassen zugeordnet werden.
- iOS erlaubt die Zusammenarbeit (Kollaboratives Arbeiten) an Dokumenten und anderen Inhaltsformaten, wenn die entsprechenden Apps dieses unterstützen. In unterrichtlichen Kontexten ist diese Art der Zusammenarbeit durchaus sinnvoll. Lehrkräfte können so Dokumente bereitstellen, an denen die ganze Klasse mitarbeiten kann.
    - Voraussetzung für die Nutzung der Funktion zur Zusammenarbeit ist iCloud, über welche die von verschiedenen Personen getätigten Bearbeitungen abgeglichen werden. iCloud setzt die Nutzung von managed Apple IDs oder privaten Apple IDs voraus, um andere zur Zusammenarbeit einzuladen. Neben den Apple eigenen Apps wie Pages, Keynote, Numbers und Notes unterstützen auch die Apps einiger Drittanbieter diese Funktionen.

Funktionalität

Ohne Einschränkungen durch das MDM steht managed Apple IDs und privaten Apple IDs die iCloud für verschiedene Funktionen zur Verfügung. Die meisten Prozesse laufen dabei automatisch und für den Nutzer unsichtbar im Hintergrund ab. Auch wenn Nutzer nicht aktiv Inhalte in iCloud speichern, werden viele Inhalte und Metadaten in die iCloud übertragen, über die Backup Funktion, die Funktion zur Zusammenarbeit, die iCloud Speicherfunktion wie auch eine Funktion, über welche diese Daten für iCloud und andere Geräte des gleichen Nutzers zur Verfügung gestellt werden (Continuity). Voraussetzung dafür ist, dass Apps diese Funktionen unterstützen. Bei vielen Apps ist das der Fall.

Datenschutz

Mit Blick auf Datenschutz sollten weder Inhalte mit personenbezogenen Daten aus der Schule noch Daten, welche personenbezogene oder -beziehbare Daten des schulischen iPad Nutzers enthalten, in der iCloud verarbeitet und/ oder gespeichert werden. Während es in der Verantwortung der Schule liegt, die personenbezogenen Daten eines Nutzers mit einer schulischen managed Apple ID zu schützen, liegt die Verantwortung für den Schutz und die Sicherheit der eigenen personenbezogenen Daten im Zusammenhang mit der Nutzung einer privaten Apple ID auf einem Dienstgerät beim Benutzer selbst. In der Verantwortung des Benutzers liegt außerdem die Umsetzung der von der Schule vorgegebenen Schutzmaßnahmen zum Schutz der von ihm auf dem Dienstgerät verarbeiteten schulischen personenbezogenen Daten, soweit diese durch die Nutzung einer privaten Apple ID auf dem Dienstgerät zusätzlich erforderlich sind.

Private Apple IDs - Vorteile

Lehrkräfte können

- Apps installieren, die ihnen von der Schule über das MDM nicht bereitgestellt werden.
- Apps installieren, die in App Käufe zulassen und keine VPP Version bieten, die alle diese Extras inkludiert.
- Apps nutzen, die sie bereits privat erworben haben.
- die Funktion zur Zusammenarbeit bei Inhalten nutzen, die keine personenbezogenen Daten enthalten.

Private Apple IDs - Nachteile

Aus Nutzersicht hat die Anmeldung über eine private Apple ID mehr Vorteile als Nachteile. Von vielen Nutzern wird jedoch als Nachteil wahrgenommen, dass sie für privat installierte Apps eigenständig Einstellungen vornehmen müssen, um Datenschutz und -sicherheit für damit verarbeitete personenbezogene Daten (sofern zulässig) zu gewährleisten. Aus Sicht der Schule ergeben sich zusätzliche Risiken bei der Verarbeitung von personenbezogenen Daten, wenn die Nutzung von privaten Apple IDs zugelassen wird.

Private Apple IDs - Risiken

Risiken können entstehen, wenn der Nutzer sich mit seiner private Apple ID am Gerät anmeldet (und nicht nur am App Store). Ist eine private Apple ID nicht ausreichend abgesichert (schwaches Passwort), können sich Dritte eventuell unberechtigt Zugriff auf die iCloud und Kontoverwaltung der privaten Apple ID verschaffen und darüber

- auf in iCloud gespeicherte bzw. synchronisierte Daten zugreifen,
- auf ein in iCloud gespeichertes Backup zugreifen und dieses auf einem fremden Gerät wiederherstellen und dadurch an auf dem iPad verarbeitete Daten gelangen,
- den Zugriff auf das iPad, die darauf gespeicherten Daten und das Nutzerkonto unterbinden,
- das iPad aus der Ferne löschen.

Risiken können bereits entstehen, wenn der Nutzer sich lediglich am App Store anmeldet, ohne dass ein Nutzer am Gerät angemeldet ist, und zusätzlich die iCloud für sich aktiviert. Diese Risiken entstehen auch, wenn der Nutzer sich direkt am Gerät anmeldet, da er dann auch zum App Store Nutzer wird. Apps, die durch eine private Apple ID installiert werden, unterliegen bezüglich iCloud nicht automatisch den Einschränkungen von verwalteten Apps. Datenflüsse zu anderen mit privat installierten Apps verbundenen Online-Diensten lassen sich nicht durch Einschränkungen steuern. Risiken können entstehen, wenn

- mit diesen nicht verwalteten Apps personenbezogene Daten aus der Schule verarbeitet werden und eine Speicherung in iCloud nicht durch den Nutzer unterbunden wird,
- verwaltete Apps, mit denen personenbezogene Daten verarbeitet werden, Daten an nicht verwaltete Apps weitergeben können, bzw. nicht verwaltete Apps, Zugriff auf die in verwalteten Apps verarbeiteten personenbezogenen Daten haben,
- personenbezogene Daten aus nicht verwalteten Apps an mit diesen verbundene Online-Dienste abfließen.

Eine Quelle weiterer Risiken ist die Installation von Apps, welche die Sicherheit und den Schutz der auf dem Gerät verarbeiteten Daten gefährden,

- wenn sie Schadcode enthalten, der es ihnen ermöglicht, auf von anderen Apps verarbeitete Daten zuzugreifen und sie zu manipulieren, zu löschen oder an Dritte zu übermitteln,
- wenn Benutzer ihnen durch Fehleinschätzungen Berechtigungen geben, welche ihnen Zugriff auf von anderen Apps verarbeitete Daten geben.

Managed Apple IDs - Vorteile

Managed Apple IDs haben Vorteile in zwei Bereichen. Auf der einen Seite sind spezielle Funktionen wie Apple Schoolwork und ein Speicherkontingent von 200 GB in iCloud, die nur managed Apple IDs zur Verfügung stehen. Und auf der anderen Seite sind es Einschränkungen, welchen managed Apple IDs durch iOS unterworfen sind. Diese erhöhen die Sicherheit und reduzieren das Missbrauchspotential. Deshalb können managed Apple IDs im App Store und in iTunes keine Käufe tätigen und es stehen ihnen Dienste wie “Find my” und “Apple Pay” nicht zur Verfügung. Im App Store können sie lediglich verfügbare Apps installieren und aktualisieren, soweit der App Store nicht unterdrückt ist. Der Login an iCloud ist von jedem Gerät aus möglich, setzt aber einen sechsstelligen, von der Schule bereitgestellten Bestätigungscode voraus. Dieser Code ist ein Jahr lang gültig. Gibt der User beim Login an einem Browser an, dem Browser zu vertrauen, muss der Bestätigungscode für diesen Browser auf dem Gerät erst wieder eingegeben werden, wenn sich die öffentliche IP ändert. Mit der managed Apple ID, Passwort und Bestätigungscode können Nutzer sich auch an einem nicht-schulischen Apple Gerät anmelden.

Managed Apple IDs - Nachteile

Ähnlich wie bei privaten Apple IDs haben managed Apple IDs ohne entsprechende Einschränkungen vollen Zugriff auf die Funktionen der iCloud (Synchronisation, Backup, Speicherung, Zusammenarbeit). Anders als private Apple IDs können sie weder Apps im App Store kaufen, noch zu vorhandenen Apps in App Käufe tätigen. Eine Ausnahme besteht nur für managed Apple IDs, die über ASM eine Funktion zugewiesen bekommen haben, welche ihnen App Käufe im VPP Store der Schule erlauben. In iCloud ist kein iCloud Mail verfügbar. Ohne Bestätigungscode ist eine Anmeldung in iCloud oder an nicht-schulischen Geräten nicht möglich. Bei schulischen Geräten wird ein Bestätigungscode für die Anmeldung benötigt, sobald sich seine öffentliche IP Nummer ändert. Einschränkungen der iCloud durch das MDM wirken ähnlich wie auch bei Anmeldung mit einer privaten Apple ID nicht auf die System-Apps. Diese nutzen die Funktionen der iCloud, solange die managed Apple ID iCloud nicht manuell für jedes System-App deaktiviert.

Managed Apple IDs - Risiken

Ohne Setzen der entsprechenden Einschränkungen im MDM können von Lehrkräften verarbeitete personenbezogene Daten aus der Schule von allen verwalteten Apps, welche die iCloud Funktionen (Synchronisation, Backup, Speicherung, Zusammenarbeit) unterstützen, in iCloud gespeichert werden. Das gilt auch für die System-Apps, solange der Nutzer der managed Apple ID die iCloud für diese Apps nicht manuell deaktiviert.

Durch die Einschränkungen, welchen managed Apple IDs unterliegen, sind sie auch ohne zusätzliche Maßnahmen etwas besser abgesichert als private Apple IDs. Ein Zugriff auf iCloud und appleid.apple.com (Kontoverwaltung) ist nur mit dem von der Schule vergebenen sechsstelligen Bestätigungscode möglich und die Funktionen von iCloud sind reduziert. Meldet sich eine managed Apple ID über den Browser auf einem beliebigen Computer in iCloud an und speichert dort die Zugangsdaten oder meldet sich nach der Sitzung nicht wieder ordnungsgemäß ab, ist es auch für Dritte möglich, auf die Inhalte der iCloud zuzugreifen, diese herunterzuladen, zu verändern oder zu löschen. Je nach Einstellung auf dem iPad wirkt sich dieses dann auch auf die dort gespeicherten Daten aus.

Unter appleid.apple.com kann das Passwort des Kontos geändert werden. Damit Dritte dieses tun können, benötigen sie neben der managed Apple ID, deren Passwort und den Bestätigungscode, um sich dort anzumelden. Vergisst der Nutzer, sich von appleid.apple.com abzumelden, wird er nach wenigen Minuten Inaktivität automatisch abgemeldet. Ein Löschen des Gerätes über iCloud oder Apple Konto ist für Dritte, die sich unberechtigt Zugang verschafft haben, nicht möglich, da die Funktion “Find my”, die dafür erforderlich ist, für managed Apple IDs nicht zur Verfügung steht.

Empfehlung - Apple IDs

Vielfach steht bei Schulen und Schulträgern die Frage im Raum, ob es Gründe gibt, die gegen eine Nutzung von Apple IDs sprechen. Die Antwort darauf ist für Niedersachsen kurz - ja. Mit Blick auf das geltende Schutzstufenkonzept ist anzunehmen, dass Nutzer:innen des Gerätes grundsätzlich personenbezogenen Daten mit sehr hohem Schutzbedarf verarbeiten.

Anmeldung mit Apple IDs

Bei der Anmeldung an einem iPad ist zwischen zwei Anmeldungen zu unterscheiden, der Anmeldung am Gerät und der Anmeldung am App Store.

Anmeldung am Gerät

Die Anmeldung am Gerät erfolgt über “Einstellungen”. Damit erhält die angemeldete Apple ID automatisch Zugriff auf alle Apple Dienste auf dem Gerät, sofern diese nicht durch Einschränkungen im MDM unterbunden sind. Mit der Anmeldung am Gerät ohne Einschränkungen ist die Apple ID auch direkt an iCloud angemeldet und kann den App Store aktivieren und iTunes. Eine komplette Deaktivierung der iCloud durch den Nutzer ist bei dieser Art der Anmeldung nur durch ein Abmelden vom Gerät möglich. Alternativ muss die iCloud Einbindung für jedes App einzeln deaktiviert werden. In dem Fall muss der Nutzer auch iCloud Drive und die Backup Funktion manuell deaktivieren.

Anmeldung im App Store und bei iTunes

Keine managed Apple IDs am Gerät angemeldet

Alternativ zur Anmeldung am Gerät über die “Einstellungen” besteht die Möglichkeit, sich mit einer privaten Apple ID direkt am “App Store” anzumelden. Im Unterschied zu einer Anmeldung am Gerät ist in diesem Fall die iCloud noch nicht aktiviert und erfordert eine manuelle Aktivierung durch den Nutzer. Angezeigt werden dazu beim ersten Anklicken des Menüpunkts iCloud die Optionen “Aktivieren” und “Später”. Die Aktivierung ist durch Eingabe eines Passwortes geschützt. Funktionen der iCloud stehen für die vom Nutzer installierten Apps wie auch die System-Apps und verwaltete Apps erst dann zur Verfügung, wenn dieser die iCloud aktiviert. Bis dahin findet kein Datenaustausch dieser Apps mit iCloud statt.

Managed Apple ID bereits am Gerät angemeldet

Eine direkte Anmeldung am App Store ist auch dann möglich, wenn der Nutzer bereits mit seiner managed Apple ID am Gerät angemeldet ist. Die managed Apple ID kann vom App Store dazu abgemeldet werden und der Nutzer meldet sich mit einer privaten Apple ID dort an. Über diese private Apple ID lassen sich dann Apps installieren und kaufen. Durch die managed Apple ID ist die iCloud bereits belegt. Dadurch können die vom Nutzer der privaten Apple ID installierten Apps nicht auf die iCloud Funktionen der eigenen iCloud zugreifen. Bei aktivierter iCloud der am Gerät angemeldeten managed Apple ID ist es jedoch möglich, dass die Daten aus den nicht verwalteten Apps in die iCloud der managed Apple ID synchronisiert werden, wenn die dafür erforderlichen Einschränkungen (engl. payloads) zugelassen sind. Nutzer sollten deshalb die iCloud für die von ihnen installierten Apps auf jeden Fall deaktivieren. Gleiches gilt für die der managed Apple ID zugeordneten System-Apps. Hier muss die iCloud manuell durch den Nutzer deaktiviert werden. Hinweis: werden in dieser Konstellation von managed Apple ID und privater Apple ID Apps privat installiert, kann das MDM diese zwar in Bezug auf die Berechtigungen für verwaltete und nicht verwaltete Apps unterscheiden, wird aber bei einer Neuinstallation durch das MDM nicht verwaltete Apps “überschreiben” (bzw. in verwaltete Apps umwandeln)

und dabei bestehende Inhalte übernehmen.

Um den Abfluss von personenbezogenen Daten in die iCloud zu unterbinden, ist die direkte Anmeldung über den App Store ohne anschließende Aktivierung der iCloud der einfachste Weg, dieses Ziel zu erreichen.