Bayerisches Staatsministerium für
Unterricht und Kultus

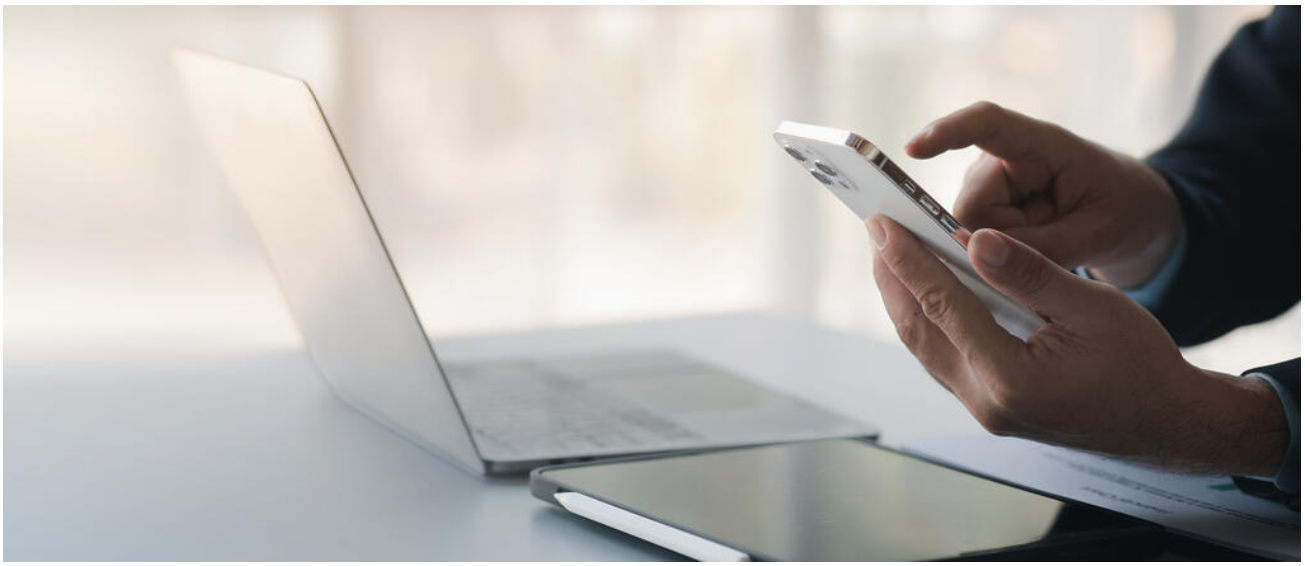
Mobile Device Management

Stand: 28.01.2026

→ www.km.bayern.de / gestalten / digitalisierung / datensicherheit / mobile-device-management

Inhaltsverzeichnis

Mobile Device Management



Durch Mobile Device Management lässt sich Geräteverwaltung vereinfachen. ©PhotosD - stock.adobe.com

Allgemein

Ein Mobile Device Management (MDM-System) ist eine zentrale Anwendung zur Verwaltung mobiler Endgeräte wie Tablets oder Laptops. Mit einem MDM-System können IT-Verantwortliche mobile Endgeräte aus der Ferne konfigurieren, steuern und absichern. Dies umfasst unter anderem

- die Ersteinrichtung und Inventarisierung der Geräte,
- die Konfiguration der Geräte,
- das Einrichten von Netzwerkzugängen,
- die zentrale Installation und Deinstallation von Anwendungen (Apps) sowie
- das Verteilen von System- und Softwareupdates.

Ein wesentlicher Vorteil beim Einsatz eines MDM-Systems liegt in der Effizienz und Sicherstellung der passgenauen Geräteeinstellungen. MDM-Systeme ermöglichen es, unterschiedliche Nutzergruppen – wie beispielsweise Schüler und Lehrkräfte – mit maßgeschneiderten Profilen auszustatten. Während Schülergeräte während der Unterrichtszeit beispielsweise nur eingeschränkt nutzbar sind, behalten Lehrkräfte vollen Zugriff auf ihre digitalen Werkzeuge. Gleichzeitig kann das MDM-System Daten, etwa durch die Möglichkeit, verlorene Geräte zu sperren oder zu löschen, schützen. Auch

datenschutztechnische Anforderungen lassen sich mit einem MDM einfacher erfüllen, da beispielsweise private und schulische Inhalte strikt voneinander getrennt werden und die Geräte gemäß dem Prinzip der Datensparsamkeit konfiguriert werden können. Eine Verwaltung der Endgeräte durch die Schule selbst ist ebenso denkbar wie die Verwaltung durch den Schulaufwandsträger oder einer beauftragten Firma.

Hinweis

Entgegen der verbreiteten Meinung ist über ein MDM-System kein Zugriff auf lokal oder in einer Cloud gespeicherte Inhaltsdaten, wie Fotos, Videos, Browser- und Suchverläufe, private Dokumente o. ä. möglich. Auch die Inhalte von App-Daten (z.B. Chats) können über ein MDM-System nicht eingesehen werden.

Trotz dieser Vorteile bringt der Einsatz von MDM-Systemen auch einige Herausforderungen mit sich. An Schulen müssen technische Lösungen mit pädagogischen Anforderungen und Datenschutzrichtlinien in Einklang gebracht werden.

Die Einrichtung und Pflege eines MDM-Systems erfordert nicht nur technisches Know-how, sondern auch klare Abstimmungen innerhalb der Schulfamilie, sowie zwischen der Schulleitung, den IT-Verantwortlichen und Schulaufwandsträgern. Auch die Vielfalt der eingesetzten Endgeräte und Betriebssysteme stellt Schulen vor die Aufgabe, einheitliche Standards zu schaffen, ohne die individuelle Nutzung zu stark zu begrenzen.

Checkliste und Dokumente

Da beim Einsatz eines MDM-Systems viele verschieden Aspekte zu berücksichtigen sind, stellt das StMUK eine **Checkliste** zum Download bereit. Sie dient als Übersicht und kann gleichzeitig zu Dokumentationszwecken verwendet werden.

Zusätzlich finden sich hier auch weitere Dokumente zur **Information der Erziehungsberechtigten** zum Einsatz eines MDM.

Zielgruppe: Schulleitungen, pädagogische Systembetreuer, örtliche Datenschutzbeauftragte

Checkliste zum Einsatz eines MDM-Systems
/download/4-25-09/251106_MDM_Checkliste.jpg

Muster Elternanschreiben zum Einsatz eines MDM-Systems
/download/4-25-09/250911_MDM_Muster-Elternanschreiben.jpg

Elterninformation zum MDM
/download/4-25-09/250611_MDM_Elterninformation.jpg

Elterninformation zum MDM (einfache Sprache)
/download/4-25-09/250611_MDM_Elterninformation_einfache-Sprache.jpg

Eine **Muster-Verarbeitungsbeschreibung** ist im Schulportal hinterlegt.

Auswahl eines MDM-Systems

Im Bereich der mobilen Endgeräte gibt es unterschiedliche Betriebssystemhersteller: Insofern werden MDM-Systeme in zwei Arten eingeteilt:

- **Spezialisierte Lösungen**, die nur **ein Betriebssystem** unterstützen, und
- **Generalistische Lösungen**, die **mehrere Betriebssysteme** unterstützen.

Ein MDM-System muss zu den individuellen technischen Rahmenbedingungen der Schule passen. Diese gilt es gemeinsam mit dem Schulaufwandsträger zu analysieren, um anschließend ein für die Schule passendes System auszuwählen. Die Beratung für digitale Bildung kann dabei unterstützen.

Die verschiedenen MDM-Systeme unterscheiden sich zum Teil erheblich in ihren Funktionalitäten. Die nachfolgenden **Kriterien** an ein MDM-System sollen bei der Auswahlentscheidung unterstützen:

Kriterien zur Auswahl eines MDM-Systems

Datenschutzkonformität: Das gewählte MDM-System muss den datenschutzrechtlichen Anforderungen des Grundsatzes der Erforderlichkeit, der Rechtmäßigkeit der Datenverarbeitung, der Zweckbindung, der Datenminimierung und der Transparenz entsprechen. Zudem sollte stets geprüft werden, ob sogenannte souveräne bzw. in der EU ansässige Anbieter in Betracht gezogen werden können. Der Anbieter muss offenlegen, in welcher Form welche Drittanbieter, Sub- und Nachunternehmer an der Erbringung des

Dienstangebotes vertraglich und funktional beteiligt sind.

Möglichkeit der Registrierung von persönlichen und schulischen Endgeräten im MDM-System: Viele Betriebssysteme ermöglichen die Registrierung eines Endgeräts als persönliches Gerät in einem MDM-System, was die Trennung von privaten und schulischen Daten erleichtert. Privat installierte Apps sind dabei über das MDM i. d. R. nicht sichtbar. Für die Integration in das MDM-System sind schulische Konten erforderlich, die parallel zu privaten Konten genutzt werden können.

Funktion zur Bildung von (dynamischen) Gerätegruppen: Endgeräte werden zur Verteilung von schulischen Anwendungen und Richtlinien (Profilen) in Gerätegruppen eingruppiert. Die Zuteilung erfolgt optimalerweise automatisiert mit Hilfe von Zuordnungsregeln. Typische Gerätegruppen wären z. B. Lehrergeräte, Schülergeräte, klassenspezifische Gerätegruppen.

Möglichkeit des temporären Ausspielens von Richtlinien (z. B. Einschränkungen) auf das Endgerät während der Unterrichtszeit: Bei elternfinanzierten Endgeräten soll außerhalb der Unterrichtszeit eine private Nutzung möglich sein. Aus diesem Grund sind administrative Vorkehrungen zu treffen, damit etwaig vorhandene während der Unterrichtszeit geltende Restriktionen aufgehoben werden. Folgende Möglichkeiten stehen hierfür zur Verfügung:

- zeitgesteuert
- standortbezogen (z. B. per GPS)
- netzwerkbezogen (z. B. im schulischen WLAN)
- benutzerbezogen
- App-gesteuert

Anfallende Lizensierungskosten: Bei der Auswahl eines MDM-Systems sollte darauf geachtet werden, welche Arten von Lizenzen angeboten werden (z. B. jährliche, dauerhafte) und ob weitere Kosten (z. B. einmalig anfallende Kosten, Kosten für das Hosting) anfallen. Darüber hinaus müssen ggf. vergaberechtliche Aspekte in Abstimmung mit dem Schulaufwandsträger bedacht werden.

Möglichkeit der Nutzung einer Testumgebung: Die Verwaltung von mobilen Endgeräten ist eine administrative Tätigkeit, die eine konzeptionelle Vorarbeit erfordert. Die vorher genannten Anforderungen können nur im Rahmen einer Teststellung getestet werden und mit weiteren schulischen Anforderungen überprüft werden. Eine Teststellung ist i. d. R. über den Hersteller kostenlos einrichtbar. Teststellungen sind zeitlich oder gerätebezogen begrenzt, jedoch nicht im Funktionsumfang.

Hosting: Viele MDM-Systeme sind als reine Cloud-Lösungen konzipiert, bieten aber auch die Möglichkeit eines lokalen Betriebs in einem eigenen Rechenzentrum (On-Premises). Cloudbasierte MDM-Systeme bieten Kosteneinsparungen und Flexibilität, während On-Premises-Lösungen mehr Kontrolle und Sicherheit bieten können. Der Serverstandort soll, unabhängig vom gewählten Hosting-Modell, innerhalb Deutschlands oder der EU liegen.

optionale Funktionalitäten: Integriertes Ausleihsystem, eigene pädagogische Anwendungen, Verwaltung von weiteren Geräten, wie z. B. Displays, Möglichkeit der Konfiguration von

Anwendungen (z. B. Browser)

Zudem sind Anforderungen an die Datensicherheit zu berücksichtigen. Diese sind insbesondere die nachfolgend genannten:

Anforderungen an die Datensicherheit

Nachweis der IT-Sicherheit: Der Anbieter muss in geeigneter Form nachweisen, dass er ein Informationssicherheitsmanagementsystem betreibt. Bei Betrieb des MDM-Systems in der Cloud muss dieses auch die Sicherheit der Cloud umfassen.

Rollen und Berechtigungen: Das MDM-System soll über ein vordefiniertes Rollen- und Berechtigungskonzept verfügen. Der administrative Zugriff soll granular einstellbar sein, damit auch verschiedene Berechtigungsstufen abgebildet werden können.

Sichere Authentifizierung: Authentifizierungsvorgänge müssen mittels MFA möglich sein und dürfen nur über TLS-verschlüsselte Kanäle erfolgen.

Mandantentrennung: Der Anbieter muss bei Nutzung die vollständige Trennung der mandantenbezogenen Daten gewährleisten.

Patchmanagement: Der Anbieter muss gewährleisten, dass sicherheitsrelevante Updates (Sicherheitspatches) für Komponenten in seinem Verantwortungsbereich zeitnah eingespielt werden.

Betrieb eines MDM-Systems

Konfiguration des MDM-Systems

Bei der Inbetriebnahme muss die Schule ggfs. in Abstimmung mit dem Schulaufwandsträger oder einem externen Dienstleister ein Rollen- und Berechtigungskonzept nach dem → „Least Privilege“ und „Need to know“ Prinzip https://www.km.bayern.de/gestalten/digitalisierung/datensicherheit/berechtigungsmanagement festlegen. Bei einem Mehrmandanten-Einsatz muss sichergestellt werden, dass eine klare Trennung zwischen den Mandaten stattfindet. Administratoren eines Mandaten dürfen keine Daten eines anderen Mandaten sehen können. Ausnahmen hiervon sind z. B. für Administratoren möglich, die mehrere Mandanten zentral verwalten.

Der Zugriff auf die (Web-)Oberfläche des MDM-Systems muss nach aktuellen Sicherheitsstandards erfolgen. Für Administratoren muss eine Zwei-Faktoren-Authentifizierung verfügbar sein. Um Zugriff auf App-Marktplätze zu erhalten, muss das MDM-System mit dem Bildungsaccount der Schule bei den Betriebssystemherstellern verbunden werden.

Registrierungsmöglichkeiten der Endgeräte im MDM-System

Bei der Registrierung der mobilen Endgeräte im MDM-System (dem Enrollment) sind grundsätzlich zwei Möglichkeiten zu unterscheiden:

- Registrierung als schuleigenes Gerät (Umfängliche Verwaltung oder Vollverwaltung)
- Benutzergesteuerte Registrierung als persönliches Gerät (Eingeschränkte Verwaltung oder Teilverwaltung)

Daraus ergeben sich verschiedene Steuerungsmöglichkeiten, die im Folgenden kurz dargelegt werden sollen.

Enrollment als schuleigenes Endgerät (z. B. Leihgeräte, Lehrergeräte, Ausbildungsgeräte)

Bei der Vollverwaltung wird das Endgerät umfangreich durch die Schule bzw. den Schulaufwandsträger verwaltet. Im Normalfall wird es zuerst im zentralen Bildungsaccount der Schule hinterlegt. Anschließend werden die Endgeräte automatisch im MDM-System der Schule registriert und können anschließend umfangreich verwaltet werden. Der Nutzende kann normalerweise nicht eigenständig die MDM-Verwaltung verlassen. Es sind dann u. a. folgende administrative Tätigkeiten möglich:

Automatische Ersteinrichtung des Endgeräts („Zero-Touch“) Installation von Betriebssystemupdates Installation von Anwendungen und -updates Ausspielen von Gerätekonfigurationen (z. B. Netzwerkeinstellungen, notwendige Zertifikate) Installation von befristeten Geräteeinschränkungen Ausblenden von nicht-unterrichtlichen Anwendungen Zurücksetzen und Neueinrichtung des mobilen Endgeräts Lösen von Gerätesperrungen (z. B. per Bildschirmcode) Remote-Sperren und Orten des (mobilen) Endgeräts

Benutzergesteuertes Enrollment (z. B. für private bzw. elternfinanzierte Geräte)

Das mobile Endgerät wird als persönliches Endgerät mit Hilfe eines schuleigenen Benutzerzugangs beim MDM-System der Schule direkt registriert. Das Betriebssystem richtet dann einen persönlichen und schulischen Bereich ein, die voneinander getrennt sind. Über das MDM können dann u. a. folgende administrative Tätigkeiten ausgeführt werden:

Installation von Anwendungen und -updates Installation von Betriebssystemupdates Ausspielen von Gerätekonfigurationen (z. B. Netzwerkeinstellungen, notwendige Zertifikate) Installation von befristeten Geräteeinschränkungen

Das Verlassen des MDM-Systems ist jederzeit möglich. Eine Zurücksetzung des mobilen Endgeräts ist nicht notwendig. Schulische Daten sollten vorher gesichert werden, da es ansonsten zu einem Datenverlust kommen kann. Nach dem Verlassen des MDM-Systems ist der Zugriff auf die schulischen Anwendungen nicht mehr möglich, und diese werden vom mobilen Endgerät automatisch entfernt.

Zusammenspiel zwischen MDM-System und Schulkonten der Betriebssystemhersteller

Für eine sinnvolle Administration der mobilen Endgeräte ist ein entsprechender Bildungsaccount bei den Betriebssystemherstellern (z. B. Apple School Manager, Google Workspace und Microsoft 365 Tenant) anzulegen. Dadurch erhält die Schule Zugriff auf die herstellereigenen App-Marktplätze, der für die Verteilung der Anwendungen an die mobilen Endgeräte Voraussetzung ist. Die Schule erhält so die Möglichkeit von Bildungsrabatten zu profitieren und kann Volumenlizenzen für Anwendungen erwerben. Die mobilen Endgeräte sollten bei einem zertifizierten Bildungshändler des Betriebssystemherstellers gekauft werden, da diese Händler dazu berechtigt sind, die beschafften mobilen Endgeräte direkt im Bildungsaccount zu hinterlegen und fest mit diesem zu verknüpfen. Ebenfalls kann über diese Händler auch notwendiges Guthaben für den Kauf von kostenpflichtigen Anwendungen aus dem App-Store erworben werden.

Innerhalb der Schulaccounts können schuleigene Cloud-Accounts zur Anmeldung auf den mobilen Endgeräten eingerichtet und verwaltet werden. Hierbei sind die datenschutzrechtlichen Anforderungen zu beachten.

Das gewählte MDM-System wird mit dem Bildungsaccount der Schule verbunden. Anschließend können die hinterlegten Endgeräte, die lizensierten Anwendungen sowie etwaige Schulaccounts dem MDM zur zentralen Verwaltung zugewiesen werden. Es ist darauf zu achten, dass die notwendigen Zertifikate (Tokens) und Lizenzen rechtzeitig erneuert werden. Die Kommunikation zwischen Bildungsaccount und MDM-System erfolgt

verschlüsselt.

Entfernen von Endgeräten aus dem MDM-System

Beim Entfernen der mobilen Endgeräte aus dem MDM-System muss wieder zwischen voll- bzw. teilverwalteten Geräten unterschieden werden.

Vollverwaltete Endgeräte sind stärker mit der MDM-Lösung und dem Bildungsaccount verzahnt, weswegen eine Loslösung nicht ohne weiteres möglich ist und eine Zurücksetzung des mobilen Endgeräts regelmäßig erforderlich ist. Deswegen sollten zuerst lokal gespeicherte Daten vom mobilen Endgerät gesichert werden. Anschließend wird das mobile Endgerät auf die Werkseinstellungen zurückgesetzt und alle Daten vom Endgerät gelöscht (Enterprise-Wipe). Das kann über das MDM oder manuell am Endgerät über die Rücksetzungsfunktionen erfolgen. Im nächsten Schritt wird das mobile Endgerät aus dem MDM und dem Bildungsaccount der Schule gelöscht.

Bei **teilverwalteten Endgeräten** kann das MDM-System direkt, durch Entfernen des Schulaccounts verlassen werden.

Konfiguration der Endgeräte

Endgeräte sollen so konfiguriert sein, dass sie das erforderliche Schutzniveau angemessen erfüllen. Dafür muss eine passende Grundkonfiguration der Sicherheitsmechanismen und -einstellungen zusammengestellt und dokumentiert werden. Nicht benötigte Funktionen sollten deaktiviert werden.

Die untenstehende Excel-Tabelle bildet für verschiedene Endgeräte Konfigurationsempfehlungen ab. Die Tabelle kann an die Gegebenheiten der Schule angepasst und beispielsweise ergänzend dem Elterninformationsschreiben als Anhang hinzugefügt werden.

Zielgruppe: pädagogischer Systembetreuer, MDM-Administrator

Konfigurationsempfehlungen für verschiedene Endgeräte
/download/4-25-09/250911_MDM_Ger%C3%A4tekonfiguration.jpg

FAQ zu MDM-Systemen

Welche Arten von Konten können für die Anmeldung auf Endgeräten verwendet werden?

Zur Anmeldung auf Endgeräten (z. B. Notebook, Desktop-PC, Tablet) kommen **Cloud-Konten** und **lokale Konten** in Frage.

Cloud-Konten können bei Microsoft (Windows), Apple (iPadOS, macOS) oder Google (Android, ChromeOS) für die Anmeldung auf dem Endgerät angelegt werden.

Lokale Konten können für Windows, Linux oder macOS angelegt werden.

Welche Konten kommen in windowsbasierten Domänen zum Einsatz?

Windows-basierte Endgeräte werden im Schulumfeld häufig in Windows-Domänen eingebunden und werden damit Teil eines lokalen Verzeichnisdienstes (Active Directory). Diese Strukturen können über den Entra-Connect-Dienst auch mit dem Cloud-Identitätsdienst Microsoft Entra aus der Microsoft-Cloud verbunden werden. Die lokalen Benutzerkonten aus dem Active Directory werden anschließend in die Cloud synchronisiert und können für die Anmeldung an Windows und den Microsoft365-Diensten verwendet werden.

Welche Arten von Cloud-Konten gibt es und welche Unterschiede zwischen Ihnen bestehen?

Bei Cloud-Konten kann zwischen **persönlichen** und **schulischen Konten** unterschieden werden. Ein persönliches Cloud-Konto wird mit einer persönlichen Mail-Adresse von den Nutzenden selbstständig angelegt. Die Verwaltung des Kontos liegt in der Verantwortung des Nutzenden. Neben der Anmeldung auf dem Endgerät dienen persönliche Konten als Zugang zu herstellereigenen Apps-Stores, können für Familienfunktionen oder zur Anmeldung bei Herstellerdiensten (z. B. Cloud-Dienste oder zur Ortung des eigenen Endgeräts) verwendet werden.

Schulische Cloud-Konten werden von der Schule mit einer schulischen Mail-Adresse angelegt. Die Verwaltung des Kontos wird durch die zuständige IT-Administration der Schule sichergestellt. Die Konten werden zur Anmeldung auf schulischen Endgeräten verwendet und können auch zur Lizenzierung von schulischen Anwendungen eingesetzt werden. Zu

beachten ist, dass die IT-Administration keinen Zugriff auf Inhaltsdaten (z. B. Suchverläufe, Fotos oder Videos) der Nutzenden hat.

Was ist beim Einsatz eines Geräts zu beachten, welches von mehreren Personen genutzt wird?

Bei Endgeräten, die von mehreren Personen verwendet werden, gilt es, der Datensicherheit und dem Datenschutz ein besonderes Augenmerk zu schenken. So muss sichergestellt werden, dass auf sensible Daten, wie z. B. Fotos, Videos, Browser- und Suchverläufe, kein anderer Nutzer Zugriff hat. Das kann technisch durch geeignete Nutzungskonzepte, wie z. B. durch den Gastmodus erreicht werden. Bei diesem Modus werden alle während der Sitzung generierten lokale Daten nach der Abmeldung verworfen und gelöscht. Eine organisatorische Maßnahme wäre die feste Zuweisung eines (mobilen) Endgeräts an einen Lernenden. Alternativ können auch unterschiedliche personalisierte Accounts zur Anmeldung auf dem Endgerät zum Einsatz kommen. Die lokal gespeicherten Daten sind dann nur für den jeweils angemeldeten Nutzenden zugreifbar.

Was ist der Vorteil bei der Nutzung von App-Stores der Hersteller?

Die klassischen App-Stores wie der Apple App Store oder Google Play Store garantieren einen hohen Schutz durch strenge Prüfungen und Überwachung aller angebotenen Apps. Zudem erhält die Schule einen besseren Überblick über die eingesetzten Apps und profitiert von Bildungskonditionen.

Was ist der Unterschied zwischen einem MDM-System und einem Classroom-Management-System?

MDM-Systeme und Classroom-Management-Systeme werden oft in einem Atemzug genannt. Es handelt sich aber um verschiedene Werkzeuge, die unterschiedliche Aufgaben erfüllen und sich an unterschiedliche Zielgruppen richten.

Mit einem MDM-System können **IT-Verantwortliche** teilnehmende Geräte zentral verwalten – das umfasst das Einrichten, Aktualisieren, Installieren von Apps und Durchsetzen von Sicherheitsregeln für alle Tablets oder Laptops in einer Schule. MDM sorgt also dafür, dass alle Geräte grundsätzlich sicher und einsatzbereit sind.

Ein Classroom-Management-System (z. B. Apple Classroom, Veyon) richtet sich vor allem an

Lehrkräfte, um während des Unterrichts die Steuerung der Schülergeräte zu ermöglichen. Damit können zum Beispiel die Bildschirme aller Tablets auf eine bestimmte App beschränkt, einzelne Geräte gesperrt oder Bildschirminhalte von Einzelgeräten für die Klasse projiziert werden. Ziel ist es, den Unterricht zu steuern und Störungen vorzubeugen.