Bayerisches Staatsministerium für
Unterricht und Kultus



# Classroom Management

Stand: 10.03.2026

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

# Inhaltsverzeichnis

# Classroom Management

Mit Classroom-Management-Systemen den digitalen Unterricht steuern ©Drazen - stock.adobe.com

## Beschreibung eines CMS

Die zunehmende Digitalisierung macht es erforderlich auch das Classroom Management im Unterricht durch digitale Werkzeuge zu unterstützen. Classroom-Management-Systeme (CMS) haben das Ziel u. a. digitale Geräte und Anwendungen gezielt einzusetzen, Lernmaterialien niederschwellig bereitzustellen, Störung und Ablenkung im Unterricht zu reduzieren und so die aktive Lernzeit zu erhöhen.

Beispiele für CMS (nicht abschließend und keine Empfehlung des StMUK): Apple Classroom, Google Classroom, Jamf Teacher & Student, NetSupport, Relution Teacher & Student, Samsung Classroom, Schuladmin, Veyon u.v.m.

# Typische Funktionen

Folgende Funktionalitäten werden typischerweise durch ein CMS angeboten:

**Gerätesteuerung:** Steuerung von Schülergeräten (z. B. Bildschirme sperren, Lautstärke einstellen, regulieren von Anwendungen) **Inhaltsfreigabe:** Präsentation von Inhalten per (drahloser) Bildschirmübertragung **Dokumentenverteilung:** Digitales austeilen und ggf. Einsammeln von Unterrichtsdokumenten **Monitoring**: Überblick über die Aktivitäten der Lernenden auf ihren Endgeräten, um den Unterricht zu strukturieren und Störungen zu vermeiden und unterrichtsfremde Aktivitäten zu erkennen und zu ggf. unterbinden

## Hinweise

- Es muss klar zwischen CMS und MDM unterschieden werden. Vorallem im Hinblick auf die Einsatzzwecke und die verarbeiteten Daten. Es gibt zwar Lösungen die beide Systeme integrieren, dies ist aber nicht zwingend der Fall.
- Ein CMS ist keine sicherheitsrelevante Anwendung im Sinne der IT-Sicherheit

# Technische Anforderungen und Voraussetzungen

Je nach eingesetztem CMS unterscheiden sich die Anforderungen an die schulische IT Infrastruktur. Dabei lassen sich drei Architekturen unterscheiden:

- **Lokaler Server :** Diese CMS (häufig für Windows) agieren über einen lokal betriebenen Server. Lehrer und Schülergeräte sollten sich dabei nach Möglichkeit im selben Netzwerksegment befinden, um eine zuverlässige gegenseitige Erkennung sowie die erforderliche Kommunikation zwischen den Endgeräten sicherzustellen.
- **Drahtlose Konnektivität:** Bei diesen CMS wird die Kommunikation direkt zwischen den erkannten Endgeräten abwickeln. Hierfür sind an den Endgeräten die entsprechenden Drahlosschnitstellen (WLAN, Bluetooth o. ä.) zu aktivieren.
- **Cloudbasiert:** Bei cloudbasierten CMS werden die Steuerungsbefehle über sogenannte cloudbasierte Relay Dienste vermitteln, sodass die Geräte auch ohne unmittelbare Nähe oder gemeinsames Netzwerksegment miteinander interagieren können. Dabei kann es erforderlich sein die entsprechenden Kommunikationsports an der Firewall freizuschalten.

Grundsätzlich ist auf die **Kompatibilität der Betriebssysteme** mit dem CMS zu achten. Die meisten CMS-System müssen als Anwendung (Lehrer- bzw. Schüler-App) auf den Geräten installiert werden und sind im Sinne der IT-Sicherheit regelmäßig zu patchen.

CMS verwenden in der Regel Nutzer-Konten, in den standardmäßig die Rolle Lehrer und Schüler definiert sind. Für Administratoren ist häufig eine eigene Oberfläche vorhanden in der Schüler-Konten zu Klassen angelegt werden und Lehrern-Konten entsprechende Klassen zugewiesen werden können. Sind den Lehrern-Rollen durch das CMS grundsätzlich weitreichende Rechte zum Eingriff auf das Schülergerät gestattet, müssen hier entsprechende Anpassungen vorgenommen und beispielsweise Zeiten festgelegt werden, in denen dies Eingriffe nicht möglich sind.

# Sicherer administrativer Betrieb eines CMS-Systems

Einige CMS-Lösungen verfügen über eigene Administrationsoberflächen (z. B. zum Verwalten der möglichen Gerätefunktionen, Benutzerzugänge), die besonders geschützt werden müssen. Der Zugang zu der Oberfläche ist durch eine Multi-Faktor-Authentifizierung für die Administratoren abzusichern. Sofern eine externe Verbindung von außerhalb des Schulnetzwerks auf die Adminoberfläche möglich ist, muss diese verschlüsselt (z. B. per HTTPS) erfolgen.

Einige CMS-Lösungen funktionieren auch außerhalb des gleichen Netzwerksegments. Hierfür bieten die administrativen Oberflächen die Möglichkeit, dass bestimmte Zeiten festgelegt werden, zu denen alle Einschränkungen durch Lehrkräfte von den mobilen Endgeräten gelöst werden und der Unterricht automatisch beendet wird.

# Plattformspezifische Besonderheiten der CMS

Die meisten Classroom-Management-Systeme sind an ein Betriebssystem gebunden und greifen tief in die jeweilige Plattform ein. Plattformübergreifende Lösungen sind in ihrem Funktionsumfang teilweise beschränkt und bieten nicht immer den vollen Funktionsumfang in den einzelnen Betriebssystemen.

### iPadOS / macOS

Die Endgeräte der Lehrkraft und der Schüler müssen sich i. d. R. im gleichen Netzwerk befinden und sich in Bluetooth-Reichweite befinden, damit sie sich finden. Die Lehrkraft kann dann auf spezielle Classroom-Schnittstellen des Betriebssystems zurückgreifen, um z. B. eine Bildschirmfreigabe per AirPlay oder den Start bzw. das Sperren von konkreten Apps zu

forcieren. Sie kann auch im Bedarfsfall konkrete Funktionen (z. B. Kamera) sperren.

## Windows

Die Endgeräte der Lehrkraft und der Schüler sollen sich im gleichen Netzwerk befinden. Die meisten CMS-Systeme im Windows-Umfeld setzen auf eine Client-Server-Infrastruktur (z. B. lokale Domäne) auf. Das Endgerät kann Teil einer zentralen Verzeichnisstruktur (z. B. Active Directory) sein. Regelmäßig wird auf den Lehrer- und Schülergeräten eine entsprechende Anwendung des CMS installiert, die zur Steuerung der Geräte erforderlich ist. Durch die Anmeldung am Endgerät oder direkt an der Anwendung mit den schuleigenen Benutzerzugängen werden Lehrer- und Lernende identifiziert. Anschließend werden entsprechende Schnittstellen von Windows oder eigene Dienste genutzt, um beispielsweise Bildschirmfreigabe oder -sperrung durchzusetzen, Anwendungen zu starten oder zu blockieren oder den Internetzugang temporär zu deaktivieren.

## Android

Da es eine Vielzahl von unterschiedlichen Android-Versionen gibt, ist die Funktionsweise jeweils etwas unterschiedlich. Die Endgeräte der Lehrkraft und der Schüler sollten sich im gleichen Netzwerk befinden. Die Geräteerkennung zwischen Lehrkraft und Schüler erfolgt je nach CMS unterschiedlich (z. B. per QR-Code, Klassenlisten). Die Lehrkraft kann beispielsweise Apps sperren, Bildschirmfreigeben oder die Kamera deaktivieren. Teilweise werden für die verschlüsselte Übertragung der Befehle Cloud-Dienste verwendet oder laufen auch lokal direkt zwischen den Endgeräten. Je nach gewählter Anwendung kann es erforderlich sein, dass sich Lehrkräfte und Lernende an der Anwendung mit schuleigenen Zugängen anmelden.

## ChromeOS

Die Geräte sind i. d. R. über ein Google Workspace-Konto verwaltet und innerhalb der Google Admin Konsole in die dortige Struktur eingebunden. Anhand der dort festgelegten Hierarchie sehen Lehrergeräte die entsprechenden Schülergeräte. Die Befehle zur Steuerung des Endgeräts laufen verschlüsselt über die Cloud und nutzen die Google-Dienste zur Synchronisierung. Die Lehrkraft hat die Möglichkeit beispielsweise Tabs zu schließen oder öffnen, die Bildschirmfreigabe zu starten oder den App-Zugriff einzuschränken.

# FAQ

### Welche Daten werden durch CMS verarbeitet?

Für ein CMS werden i. d. R. individuelle Benutzerzugänge für Schüler und Lehrkräfte sowie Klassenlisten benötigt, die im jeweiligen System hinterlegt werden. Die Nutzer werden anschließend in der jeweiligen Rolle (z.B. Lehrer, Schüler) der Klasse zugewiesen. Je nach gewähltem System kann es sich dabei um Cloud-Konten handeln, die auf externen Servern gespeichert werden.

Im Unterricht kann die Lehrkraft die Klasse auswählen und den Unterricht in der Anwendung starten. Die Schülerinnen und Schülergeräte erscheinen dann in einer Übersicht auf dem Lehrergerät und können gesteuert werden.

### Welche Daten werden während der Gerätesteuerung übertragen?

Zwischen den Endgeräten werden im Normalfall nur Statusdaten (z. B. aktive App, Bildschirmansicht, verwendete Anwendungen) verschlüsselt übertragen. Hierfür bauen die Endgeräte oftmals eine direkte Verbindung (ad hoc) zueinander auf ohne die Einbindung von externen Servern.

Am Ende der Unterrichtseinheit kann sich je nach System die Lehrkraft die während des Unterrichts genutzten Anwendungen der Schülerinnen und Schüler anzeigen lassen. Die Übersicht der verwendeten Anwendungen wird i. d. R. nicht dauerhaft gespeichert und ist nur am Ende der Unterrichtszeit sichtbar. Die technische Einsicht in die gewählten Anwendungen am Ende ersetzt jedoch nicht die aktive Aufsicht der Lehrkraft während der Unterrichtszeit, um bereits dort unterrichtsfremde Aktivitäten erkennen zu können.

### Kann ein Lehrer auch außerhalb des Unterrichts auf das Schülergerät zugreifen?

Voraussetzung für eine zuverlässige Steuerung der Endgeräte ist, dass sich Lehrer und Schülergeräte nach Möglichkeit im selben Netzwerksegment und – sofern vom jeweiligen System vorgesehen – zusätzlich in BluetoothReichweite befinden. Andernfalls kann es dazu kommen, dass die Geräte nicht eindeutig erkannt werden oder keine Kommunikation aufgebaut werden kann. Ein Zugriff auf Schülergeräte ist grundsätzlich nur dann möglich, wenn die Lehrkraft den Unterricht aktiv innerhalb des ClassroomManagementSystems startet und sich die beteiligten Geräte im vorgesehenen technischen Kontext befinden;

Ein Zugriff der Lehrkraft außerhalb des Unterrichts ist abhängig von dem gewählten CMS-System möglich. Insbesondere bei Systemen, die einen Client-Agenten auf Schülerendgeräten installieren, ist oftmals der Zugriff auch außerhalb des Schulhauses möglich. Deswegen können i. d. R. bei derartigen Systemen in den administrativen Oberflächen entsprechende Zeiten definiert werden, ab denen alle Einschränkungen durch eine Lehrkraft automatisch gelöscht werden.

### Kann eine Lehrkraft über ein Classroom-Management-System auf die Inhalte auf dem mobilen Endgerät zugreifen?

Die meisten Systeme verfügen über eine Dokumentenverteilungsfunktion für die Lehrkraft, die dann Dokumente über eine Netzwerkverbindung an das mobile Endgerät der Schüler sendet. Oftmals können die Dokumente nach der Bearbeitung durch die Schüler auch wieder von der Lehrkraft eingesammelt wird. Je nach gewählter Lösung hat die Lehrkraft Zugriff auf das Dateisystem des Endgeräts. Technisch funktioniert das über einen Client-Agent, der auf das mobile Endgerät installiert wurde.

Inhalte in privaten Anwendungen sind jedoch nicht direkt über die CMS-Anwendung zugänglich. Hierzu müsste die Kontrolle über das Gerät per Remote-Steuerung übernommen werden.