Konfigurationsempfehlungen für mobile Endgeräte

Beim Pilotversuch „Digitale Schule der Zukunft“ werden schülereigene Geräte im Unterricht eingesetzt, um damit den Erwerb von „21st Century Skills“ zu unterstützen und den Fachunterricht weiterzuentwickeln. Die Geräte sind dabei Privateigentum und nicht Bestandteil des Schulvermögens. Das hat auch Konsequenzen für die Möglichkeiten der Administration.

Zur Verwaltung von *schuleigenen* Geräten nutzen Schulen mitunter ein Mobile-Device-Management-System (MDM), um Software, zentral beschaffte Apps und Richtlinienprofile an die Geräte zu verteilen. Die Richtlinienprofile können beispielsweise genutzt werden, um verschiedene WLAN-Konfigurationen an die mobilen Endgeräte zu verteilen oder um Einschränkungen an einem Gerät vorzunehmen (z. B. Verbot der Nutzung der Kamera), aber auch um Apps auf den Geräten zu installieren. Im Rahmen eines sinnvollen medienpädagogischen Einsatzes sollte immer hinterfragt werden, ob weitreichende Einschränkungen nicht dem Ziel der Vermittlung von umfangreicher Medienkompetenz entgegenläuft und dieses untergräbt.

Bei *schülereigenen* Geräten, wie sie im Rahmen des Pilotversuchs vorgesehen sind, besteht für die Pilotschulen die Möglichkeit einer zentralen Administration der Geräte nur, soweit sie ihnen von den Erziehungsberechtigten eingeräumt wird. Dies kann bei Bedarf zum förderrelevanten Mindestkriterium für mobile Endgeräte gemacht werden, vgl. Nr. 6 Sätze 7 und 8[1] sowie Anlage 1 der KMBek „Digitale Schule der Zukunft“ (Az. I.4-BO1371.0/58/56).

Bevor sich eine Schule für dieses Vorgehen entscheidet, sollte genau überlegt werden, welchen Zweck die zentrale Verwaltung verfolgt und ob es nicht andere Möglichkeiten (z. B. Nutzung der Einschränkungsmöglichkeiten der Betriebssysteme) gibt, um diese Ziele zu erreichen. Zudem sollte beachtet werden, dass mit einer zunehmenden Integration in ein MDM der administrative Aufwand zunimmt.

Sofern eine Schule die Einbindung von schuleigenen Geräten in ein schulisches MDM-System möchte, sind folgende Punkte zu beachten:

- Die MDM-Einbindung ist vorab in den „technischen Mindestkriterien“ zu definieren.
- Hierbei sollte über die konkreten Einschränkungen durch das MDM und die Zugriffsmöglichkeiten der Schule informiert werden.
- Eine zeitlich und inhaltlich ausreichende Information der Erziehungsberechtigten vor Beschaffung der Geräte ist sicherzustellen; sinnvollerweise mit Infoveranstaltung etc. Die Zustimmung zur MDM-Einbindung ist zu dokumentieren (notfalls konkludent mit der Antragstellung, wenn vorherige Information nachweisbar).
- Sofern der MDM-Dienstleister Zugriff auf personenbezogene Daten hat, muss dem MDM eine AVV zugrunde liegen.
- Ein Zugriff der Schule auf gespeicherte Daten des Endnutzers aus privater Nutzung muss möglichst ausgeschlossen sein bzw. bedarf der Einwilligung des Betroffenen.

[1] „Die Schulen legen für die zu beschaffenden mobilen Endgeräte technische Mindestkriterien fest. Hierbei werden die Schulgemeinschaft und der Schulaufwandsträger vorab in geeigneter Weise beteiligt und die Kompatibilität mit der vorhandenen und geplanten IT-Bildungsinfrastruktur der Schule berücksichtigt.“

Grundsätzlich kann zwischen **drei Szenarien** bei der Verwaltung von mobilen Endgeräten unterschieden werden:

1) Ohne Verwendung eines Managementsystems der Schule

Die Schule bindet die schülereigenen Geräte nicht in ein schuleigenes Managementsystem ein. Gewünschte und pädagogisch zielführende Restriktionen können, soweit erforderlich, mit den Mitteln der Betriebssysteme (z. B. Bildschirmzeit, Kindersicherung, Familienoptionen) an den Geräten befristet eingestellt werden. Die entsprechenden Werkzeuge der Betriebssysteme können mit einem Code geschützt werden, den z. B. die Erziehungsberechtigten selbst festlegen. So können die Beschränkungen außerhalb des Unterrichts manuell entfernt werden. Den Erziehungsberechtigten wird von der Pilotschule eine Liste an unterrichtlichen Apps bereitgestellt, die diese auf die Geräte selbst installieren sollen. Die Installation kann auch im Rahmen eines Elternabends gemeinsam durchgeführt werden. Eingriffe am Endgerät durch die Schule finden in diesem Szenario nicht statt. Classroom-Systeme können bei diesem Szenario verwendet werden. Es ist bei den eingesetzten Apps ggf. eine separate Anmeldung mit einem schuleigenen Account notwendig.

2) Teilweise Integration der mobilen Endgeräte in ein Managementsystem der Schule

Bei einer teilweisen Integration registriert der Besitzer (z. B. Erziehungsberechtigter) das Gerät z. B. mit Hilfe eines schuleigenen Benutzeraccounts selbständig bei der MDM-Lösung der Schule. In den Betriebssystemen gibt es hierfür i. d. R. entsprechende Optionen. Der registrierende Benutzer wird i. d. R. als Eigentümer des Geräts im MDM hinterlegt und das Betriebssystem trennt ggf. private Daten von Organisationsdaten. Anschließend können von Seiten der Schule auf das Gerät entsprechende Profile und Software zentral ausgespielt werden. Bei den Profilen und der Gerätekontrolle sind aber nicht alle Möglichkeiten (z. B. Einschränkung des Anschlusses externer Speichergeräte, Single-Mode-Anwendung, Neustart bzw. Herunterfahren) gegeben, die bei vollständig verwalteten Geräten möglich sind. Die Erziehungsberechtigten müssen über die entsprechenden Restriktionen vorab informiert werden und ihnen zustimmen. Zudem sollen die Profile zeitlich befristet aktiv sein (z. B. nicht an Wochenenden und in den Ferien, nur zwischen 8:00 und 13:00 Uhr etc.), damit das Gerät außerhalb der Unterrichtszeit vollumfänglich genutzt werden kann. Die Besitzer der Geräte können die teilweise Administration durch die Schule widerrufen und verlassen.

3) Vollständige Integration der mobilen Endgeräte in ein Managementsystem der Schule

Hier werden die Geräte automatisiert in der MDM-Lösung der Schule registriert und vom MDM-System als schuleigene Geräte angesehen. Dadurch ergeben sich im Vergleich zu Szenario 2 umfassendere Möglichkeiten bei der Einschränkung (z. B. Ausschalten von Sprachassistenten) und Kontrolle der Geräte (z. B. als verlorenes Gerät markieren, was es unbrauchbar macht). Dadurch können mögliche Ablenkungen im Unterricht gezielter unterbunden werden, z. B. durch Beschränkung des Internetzugriffs nur auf freigegebene Seiten. Jedoch werden dadurch ggf. medienpädagogische Erziehungsaspekte in den Hintergrund gestellt, die bei der Entscheidung zu berücksichtigen sind. Zu beachten ist weiterhin, dass eine einfache Loslösung des Geräts aus dem MDM-System ohne erhöhten administrativen Aufwand nicht möglich ist. So muss beispielsweise sichergestellt sein, dass die Daten auf dem Gerät vorher gesichert werden, da das Gerät nach dem Lösen der Verbindung mit dem MDM-System i. d. R. vollständig zurückgesetzt wird und alle Inhalte gelöscht werden. Zudem sollte sichergestellt werden, dass private und schulische Daten ausreichend getrennt werden.

Bei dieser Art der Integration werden sehr weitreichende Eingriffe am mobilen Endgerät vorgenommen; die Privatgeräte der Schülerinnen und Schüler werden technisch den schuleigenen Endgeräten gleichgestellt. Eine umfassende Aufklärung der betroffenen Erziehungsberechtigten an der Pilotschule

vor Antragstellung ist hier zwingend erforderlich. Es ist auch hier durch geeignete administrative Vorkehrungen (z. B. zeitliche Befristung des Profils) sicherzustellen, dass das Gerät außerhalb der Unterrichtszeit vollumfänglich genutzt werden kann und private Apps durch den Benutzer installiert werden können. Die Verantwortung der Funktionstüchtigkeit des Geräts liegt somit hauptsächlich bei der Schule. Bei verwalteten, schülereigenen Geräten kann dem Benutzer die Möglichkeit eingeräumt werden, Konfigurationsprofile jederzeit selbstständig zu entfernen, um dadurch wieder Vollzugriff auf sein Gerät zu erhalten. Eine ausführliche, verständliche Vorabinformation und Dokumentation der von der Schule beabsichtigten Konfigurationen und administrativen Einstellungen und eventuelle Schulungsangebote sind hier unerlässlich.

Mögliche Konfigurationsempfehlungen für schulische Endgeräte

Bei der Gerätekonfiguration ist zu beachten, dass ein MDM-System nicht alle vom Hersteller implementierten Einstellungsmöglichkeiten anbieten muss. Es kann in Ausnahmefällen erforderlich sein, dass Einstellungen auf alternative Weise oder manuell vorgenommen werden müssen. Je nach Grad der Integration der Geräte in das schulische MDM-System, können einzelne Optionen verfügbar oder nicht verfügbar sein.

Exemplarisch werden zwei Konfigurationsempfehlungen für Profile vorgestellt, die während der Unterrichtszeit aktiv sind:

Szenario 1: Weniger restriktive Konfigurationsempfehlung

Merkmal	**Empfohlene Einstellung** ☑ empfohlen ✕ nicht empfohlen ? Entscheidet Schule selbst	**Erläuterung** Die mobilen Endgeräte sind in ein pädagogisches Konzept eingebettet. Ausgehend von diesem Konzept sind die jeweiligen Einstellungen zu treffen. Die vorgestellten Grundkonfigurationen sind als Empfehlung zu verstehen. Je nach schulischer Situation, pädagogisch-didaktischem Konzept, Reifegrad der Schülerinnen und Schüler und den allgemeinen Vorgaben der Schule zur Nutzung mobiler Endgeräte kann hier abgewichen werden.
Gerätefunktionalität		
Benutzung der Kamera	☑	Für Videokonferenzen oder die Erstellung von Lernvideos ist die Nutzung der Kamera essenziell. Die Sensibilisierung der Schülerinnen und Schüler für die zulässige Nutzung der Kamera ist erforderlich.
Sprachdienste aktiviert (z.B. Cortana, Siri, Alexa)	✕	
Mikrofon aktiviert	☑	Für Videokonferenzen oder die Erstellung von Lernvideos ist die Nutzung des Mikrofons essenziell. Die Sensibilisierung der Schülerinnen und Schüler für die zulässige Nutzung des Mikrofons ist erforderlich.
Systemeigene Messenger-Dienste konfiguriert	✕	
Bildschirmaufzeichnungen zulassen	☑	Für die Erstellung von Erklärvideos sollte die Funktionalität aktiviert sein. Die Sensibilisierung der Schülerinnen und Schüler für die zulässige Nutzung dieser Funktion ist erforderlich.

App Installation durch den Benutzer erlauben	☑	Der Endbenutzer soll neben den schuleigenen Apps eigene Apps installieren und verwalten können.
App Deinstallation durch den Benutzer erlauben	?	Private Apps sollen deinstalliert werden können.
Beschränkung der Bildschirmzeit	✕	Die Konfiguration der Bildschirmzeit ist nur für vollständig verwaltete Geräte sinnvoll.
Gerätespezifische Austauschdienste (z.B. Air Drop) aktivieren	?	Bei Arbeiten im Team sind gerätespezifische Austauschdienste hilfreich, in Prüfungssituationen nicht.
Autokorrekturen verwenden	?	In Prüfungssituationen evtl. nicht gewünscht.
Suchvorschläge aktivieren	?	In Prüfungssituationen evtl. nicht gewünscht.
Diktierfunktionen zulassen	?	In Prüfungssituationen evtl. nicht gewünscht.
Bluetooth zulassen	☑	Die drahtlose Bluetooth-Schnittstelle bietet die Möglichkeit zur Verbindung mit kabellosen Geräten (z. B. Kopfhörern, Tastaturen, Stift) und wird auch für die drahtlose Bildschirmübertragung verwendet.
USB-Anschluss verwenden	☑	Es können z. B. externe Speicher an das Gerät angeschlossen werden.
Near Field Communication (NFC) aktivieren	☑	NFC wird für verschiedene Dienste verwendet (z. B. bargeldloses Bezahlen) verwendet.
Sicherheit		
Gerätesperrcode bzw. Benutzerauthentifizierung aktiv	☑	Ein einfacher Zugriff auf schulische oder private Daten auf dem Gerät wird so unterbunden. Zudem erfolgt teilweise eine Verschlüsselung der integrierten Festplatte (abhängig von OS).
Biometrische Benutzer-authentifizierung aktiv	✕	Privatgeräte werden üblicherweise biometrisch entsperrt
Zeitgesteuerte Bildschirmsperre aktiv	☑	Nach einiger Zeit sollte der Bildschirm automatisch gesperrt werden, damit kein Zugriff auf Daten auf dem Gerät möglich ist.
Password Auto Fill (nur bei vorheriger Authentifizierung) verwenden	?	Für privat verbundene Konten sinnvoll
Austausch oder Synchronisation von Passwörtern zulassen	✕	
Senden von Diagnose- und Nutzungsdaten minimieren	✕	

Veränderung der Gerätesperr-codes erlauben	☑	
Änderung, Löschung oder Hin-zufügen von Richtliniensätzen erlauben	☑	
Änderung der Accounteinstel-lungen erlauben	✕	Die Verbindung mit verwalteten Konten der Schule sollte nicht entfernt werden.
Änderung des Gerätenamens erlauben	✕	
Veränderungen an Datum- und Zeiteinstellungen	✕	
Hintergrund ändern	☑	Auf privaten Geräten sollte es möglich sein, dass der Benutzer den Hintergrund individuell anpasst.
Automatische Updates aktiviert und konfiguriert	☑	Automatische Updates sollten aktiviert sein, damit neue Sicherheits- und Funkti-onsupdates aufgespielt werden.
Start in Recovery Mode erlau-ben	✕	Ein Starten im Wiederherstellungsmodus kann zu Störungen im Unterrichtsablauf führen.
VPN-Zugänge erlauben	✕	VPN-Zugänge können zur Umgehung von schulischen Schutzmaßnahmen verwen-det werden.
Verschlüsselung des Speichers aktivieren	☑	
Anwendungen		
Herstellerspezifische Stores und Dienste erlauben	?	
Herstellerspezifische Cloud-Dienste (unter Berücksichtigung der datenschutzrechtlichen Vor-gaben) erlauben	?	Die Schule kann festlegen, welche Cloud-dienste zulässig sind.
JavaScript erlauben	☑	JavaScript erlaubt dynamische Inhalte auf Websites.
Abschalten eines Pop-Up Blo-ckers erlauben	✕	Pop-Ups treten beim Browsen im Internet auf und stören die Arbeit im Browser. Zu-dem können hier Drive-by-Downloads (z. B. Viren) gestartet werden, die die Sicher-heit des Geräts massiv gefährden.
Ortungsdienste	☑	
Dienst für das Auffinden von Geräten erlauben	?	Die Schule benötigt ein Konzept wie mit Aktivierungssperren verfahren werden soll
Druckdienste zulassen	☑	Die Schule sollte überlegen, ob sie den Schülerinnen und Schülern das Ausdru-cken gestattet.

Empfehlung 2: Umfangreichere Einschränkungen

Merkmal	**Empfohlene Einstellung** ☑ empfohlen ✕ nicht empfohlen ? Entscheidet Schule selbst	**Erläuterung** Die mobilen Endgeräte sind in ein pädagogisches Konzept eingebettet. Ausgehend von diesem Konzept sind die jeweiligen Einstellungen zu treffen. Die vorgestellten Grundkonfigurationen sind als Empfehlung zu verstehen. Je nach schulischer Situation, pädagogisch-didaktischem Konzept, Reifegrad der Schülerinnen und Schüler und den allgemeinen Vorgaben der Schule zur Nutzung mobiler Endgeräte kann hier abgewichen werden.
Gerätefunktionalität		
Benutzung der Kamera	☑	Für Videokonferenzen oder der Erstellung von Lernvideos ist die Nutzung der Kamera essentiell. Die Sensibilisierung der Schülerinnen und Schüler für die zulässige Nutzung der Kamera ist erforderlich.
Sprachdienste aktiviert (z. B. Cortana, Siri, Alexa)	✕	
Mikrofon aktiviert	☑	Für Videokonferenzen oder die Erstellung von Lernvideos ist die Nutzung des Mikrofons essenziell. Die Sensibilisierung der Schülerinnen und Schüler für die zulässige Nutzung des Mikrofons ist erforderlich.
Systemeigene Messenger-Dienste konfiguriert	✕	
Bildschirmaufzeichnungen zulassen	☑	Für Erstellung von Erklärvideos sollte die Funktionalität aktiviert sein. Die Sensibilisierung der Schülerinnen und Schüler für die zulässige Nutzung dieser Funktion ist erforderlich.
App Installation durch den Benutzer erlauben	✕	Es können nur über das MDM-System schulische Apps installiert werden.
App Deinstallation durch den Benutzer erlauben	✕	Eine Deinstallation durch den Benutzer ist nicht möglich.
Beschränkung der Bildschirmzeit	☑	Die Konfiguration der Bildschirmzeit ist nur für vollständig verwaltete Geräte sinnvoll.
Gerätespezifische Austauschdienste (z.B. Air Drop) aktivieren	?	Bei Arbeiten im Team sind gerätespezifische Austauschdienste hilfreich, in Prüfungssituationen nicht.

Autokorrekturen verwenden	✕	In Prüfungssituationen evtl. nicht gewünscht.
Suchvorschläge aktivieren	✕	In Prüfungssituationen evtl. nicht gewünscht.
Diktierfunktionen zulassen	✕	In Prüfungssituationen evtl. nicht gewünscht.
Bluetooth zulassen	☑	Die drahtlose Bluetooth-Schnittstelle bietet die Möglichkeit zur Verbindung mit kabellosen Geräten (z. B. Kopfhörern, Tastaturen, Stift) und wird auch für die drahtlose Bildschirmübertragung verwendet.
USB-Anschluss verwenden	✕	Es können keine z. B. externe Speicher an das Gerät angeschlossen werden.
Near Field Communication (NFC) aktivieren	✕	NFC wird für verschiedene Dienste verwendet (z. B. bargeldloses Bezahlen, Geräterkennung) verwendet.
Sicherheit		
Gerätesperrcode bzw. Benutzerauthentifizierung aktiv	☑	Ein einfacher Zugriff auf schulische oder private Daten auf dem Gerät wird so unterbunden. Zudem erfolgt teilweise eine Verschlüsselung der integrierten Festplatte (abhängig von OS).
Biometrische Benutzer-authentifizierung aktiv	✕	Privatgeräte werden üblicherweise biometrisch entsperrt Die individuelle Freischaltung der Funktion ist bei minderjährigen Schülerinnen und Schülern nach Einwilligung der Erziehungsberechtigten möglich.
Zeitgesteuerte Bildschirmsperre aktiv	☑	Nach einiger Zeit sollte der Bildschirm automatisch gesperrt werden, damit kein Zugriff auf Daten auf dem Gerät möglich ist.
Password Auto Fill (nur bei vorheriger Authentifizierung) verwenden	✕	Das automatische Ausfüllen von Passwörtern bei der Anmeldung (z. B. bei Webdiensten) sollte nicht möglich sein, da ansonsten ein Missbrauchspotential besteht.
Austausch oder Synchronisation von Passwörtern zulassen	✕	
Senden von Diagnose- und Nutzungsdaten minimieren	✕	
Veränderung der Gerätesperrcodes erlauben	✕	
Änderung, Löschung oder Hinzufügen von Richtliniensätzen erlauben	☑	
Änderung der Accounteinstellungen erlauben	✕	Die Verbindung mit verwalteten Konten der Schule sollte nicht entfernt werden.

Änderung des Gerätenamens erlauben	✕	
Veränderungen an Datum- und Zeiteinstellungen	✕	
Hintergrund ändern	✕	
Automatische Updates aktiviert und konfiguriert	☑	Automatische Updates sollten aktiviert sein, damit neue Sicherheitsupdates aufgespielt werden.
Start in Recovery Mode erlauben	✕	Ein Starten im Wiederherstellungsmodus kann zu Störungen im Unterrichtsablauf führen.
VPN-Zugänge erlauben	✕	VPN-Zugänge können zur Umgehung von schulischen Schutzmaßnahmen verwendet werden.
Verschlüsselung des Speichers aktivieren	☑	
Anwendungen		
Herstellerspezifische Stores und Dienste erlauben	✕	
Herstellerspezifische Cloud-Dienste (unter Berücksichtigung der datenschutzrechtlichen Vorgaben) erlauben	?	Die Schule kann festlegen, welche Clouddienste zulässig sind.
JavaScript erlauben	✕	Die Abschaltung kann dazu führen, dass Webseiten nicht mehr richtig dargestellt werden. Allerdings führt eine Deaktivierung es zu einem höheren Sicherheitsniveau.
Abschalten eines Pop-Up Blockers erlauben	✕	Pop-Ups treten beim Browsen im Internet auf und stören die Arbeit im Browser. Zudem können hier Drive-by-Downloads (z. B. Viren) gestartet werden, die die Sicherheit des Geräts massiv gefährden.
Ortungsdienste	✕	
Dienst für das Auffinden von Geräten erlauben	?	Die Schule benötigt ein Konzept wie mit Aktivierungssperren verfahren werden soll
Druckdienste zulassen	?	Die Schule sollte überlegen, ob sie den Schülerinnen und Schülern das Ausdrucken gestattet.