

Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

iOS-Tablets in schulischen IT -Systemen

Konzepte und organisatorische Voraussetzungen für den Einsatz von iOS-Tablets in Schulen
Stand 19.06.2019

paedML®

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111
70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Roland Walter
Matthias Grünler
Stephan Nowotny
Michael Stehle

Endredaktion

Wird von der Redaktion eingetragen.

Bildnachweis

Symbole von "The Noun Project" (www.thenounproject.com)

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2019

Die Nutzung dieses Handbuches ist ausschließlich für eigene Zwecke zulässig. Die Nutzung sowie die Weitergabe dieses Handbuches zu kommerziellen Zwecken wie z.B. Schulungen ist nur nach ausdrücklicher Einwilligung durch das LMZ erlaubt.

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

1.	Konzeptionelle Vorüberlegungen	6
1.1	Medienentwicklungsplanung	6
1.1.1	Organisatorischer Rahmen	6
1.1.2	Nutzungskonzepte.....	7
1.1.3	Technischer Rahmen.....	8
1.1.4	Pädagogischer Rahmen	8
1.2	Anfallende Aufgaben	9
1.3	Tablets im Schulalltag: Das sollten Sie unbedingt beachten!.....	10
2.	Technische Rahmenbedingungen	11
2.1	Vergleich der Betriebssysteme iOS und Android	11
2.1.1	iOS (Apple)	11
2.1.2	Android (Google).....	11
2.2	Verwaltung	12
2.2.1	Vorteile eines MDM-Systems.....	13
2.2.2	Auswahl und Einrichtung eines MDM-Systems	13
2.2.3	Einsatzszenarien für den Geräteeinsatz.....	13
2.2.4	Geräte-Konfiguration	17
2.2.5	App-Installation.....	18
2.3	Netzwerk	18
2.3.1	Internetanbindung	19
2.3.2	WLAN und Netzwerkinfrastruktur.....	19
2.3.3	Jugendschutzfilter	20
2.4	Aufbewahrung der Geräte	20
2.5	Caching-Server.....	20
2.5.1	iOS-Geräte	21
2.5.2	Android-Geräte.....	21
2.6	Peripherie	21
2.6.1	Drucken (iOS).....	21
2.6.2	Präsentation.....	21
2.6.3	Zubehör	22
3.	Rechtliche Rahmenbedingungen	22
3.1	Datenschutz	23

3.2	Verfahrensverzeichnisse	25
3.3	Verträge zur Auftragsdatenverarbeitung	25
3.4	Nutzungsordnungen	25
3.5	Versicherungen	25
4.	Registrierung der Geräte und Lizenzierung von Apps	25
4.1	iOS (Apple)	26
4.1.1	Apple School Manager (ASM)	26
4.1.2	Device Enrollment Program - Geräteverwaltung	26
4.1.3	Volume Purchase Program – App-Verwaltung	26
4.2	Abbildung von Schulen im School-Manager	27
4.3	Perspektive Android (Google)	29
5.	Fazit	30
Anhang A : Checkliste		32
1.	Verantwortliche	32
2.	Finanzierung	33
3.	Technische Infrastruktur	33
3.1	Netzwerkkonzept	33
3.2	Gerätehandling	33
3.3	Peripherie	33
4.	Geräteverwaltung	34
5.	Konzepte für den Unterrichtseinsatz	34
6.	Fortbildung des Kollegiums	35
7.	Besonderheiten bei Einsatzszenarien	35
7.1	1:1-Szenario	35
7.2	1:N-Szenario	35
7.3	BYOD	36
8.	Rechtliche Rahmenbedingungen	36
Anhang B : Weiterführende Links		37

Vorwort

Mit dem folgenden Dokument werden Konzepte für die Integration von Tablets in die *paedML* aufgezeigt. Dieses Dokument wendet sich an Administratoren und technisch versierte Lehrkräfte, die Tablets in *die* schulische IT einbinden wollen. Die Anleitung ist eine umfangreiche Überarbeitung unserer Anleitung „*Tablets in der paedML Linux*“ aus dem Jahr 2015. Aus dem Dokument „Beratungskonzept iPad“ der Kollegen Christian Biermann, Esat Sentürk, Jan-Eric Albrecht, Michael Stehle und Stephan Novotny wurden Anregungen in dieses Dokument übernommen.

Der Tablet-Markt wandelt sich ständig und die Verwaltung mobiler Betriebssysteme wie iOS und Android ist über Mobile Device Management (MDM) professionalisiert – und leider auch kompliziert – geworden. Mittels MDM können Sie mobile Endgeräte zentral verwalten. Eine grundlegende Einführung in technische Grundzüge der Tablet-Verwaltung und das Thema MDM finden Sie in einer Artikelserie in unserem LMZ-Portal unter (<https://www.lmz-bw.de/netzwerkloesung/fachwissen/tablets-in-der-schule/>).

Die Verwaltung von *Windows*-Tablets ist inzwischen ebenfalls über einzelne MDM-Anbieter möglich, wird hier aber nicht behandelt. Mit den in der *paedML* enthaltenen Softwareverteilungsmechanismen können *Windows*-Geräte im pädagogischen Netz verwaltet und eingesetzt werden. In der vorherigen Version dieses Dokuments enthaltene Kapitel zur Integration von *Windows*-Tablets sind in diesem Dokument nicht mehr enthalten.

In einem Modellversuch hat das LMZ im Jahr 2018 den MDM-Support an Schulen evaluiert. Die darin gemachten Erfahrungen sind in den vorliegenden Text eingeflossen. Vielen Dank an die Projektschulen, die uns dabei geholfen haben, wertvolle Erfahrungen und Erkenntnisse zu sammeln.

Während des Modellversuchs mussten wir erfahren, dass der großflächige Einsatz und die Verwaltung von *Android*-Geräten als schwierig erachtet werden kann. Gründe wie die Heterogenität des *Android*-Marktes, unregelmäßige Betriebssystem-Updates oder eine (abhängig vom MDM-System) fehlende zentrale App-Lizenz-Verwaltung führen zu einem erhöhten Aufwand bei der Betreuung der Geräte. Dies wird sich vermutlich in den nächsten Jahren ändern, da sich Google mit der Weiterentwicklung der Verwaltung von mobilen Endgeräten neben dem Consumer-Markt auch den Business-Sektor als Zielgruppe erschließt.

Die hier beschriebenen Konzepte beziehen sich vornehmlich auf *iOS*-Geräte, können aber teilweise auch auf *Android* übertragen werden.

Wir wünschen Ihnen beim Durchlesen dieses Dokumentes viele Anregungen für die eigene Praxis und viel Erfolg bei der Umsetzung Ihrer Tablet-Ideen!



Wir freuen uns immer über eine Rückmeldung zu unseren Produkten.

Wenn Sie konkrete Verbesserungsvorschläge zu dieser Anleitung oder zu technischen Rahmenbedingungen haben, nehmen Sie bitte Kontakt mit unserer Hotline auf.

1. Konzeptionelle Vorüberlegungen

1.1 Medienentwicklungsplanung

Wir empfehlen unbedingt, dass Sie sich im Vorfeld einer Investition in mobile Endgeräte Gedanken darüber machen, wie Sie die Technik in Ihren schulischen Alltag integrieren können. Kriterien des Medienentwicklungsplanes (MEP) sollten hierfür herangezogen werden. In diesem Kapitel werden Stichworte aufgeführt, die Sie bedenken sollten.

1.1.1 Organisatorischer Rahmen

Finanzierung

- Damit ein aufwändig erarbeitetes pädagogisches Konzept nicht ins Leere läuft, muss im Vorfeld eine grundsätzliche Bereitschaft des Geldgebers zur Finanzierung des Projektes abgefragt werden.
- Der finanzielle Aufwand wird steigen, sobald bauliche Maßnahmen wegen Netzwerkinfrastruktur notwendig sind.
- Mögliche Finanzierungsmöglichkeiten (Kauf, Leasing, Elternfinanzierung, ...) sind ebenso zu evaluieren, wie verschiedene Geldgeber (Schulträger, Mittel aus Schuletat, Sponsoren, Förderverein, Eltern, ...).
- Im Falle von Schülergeräten (1:1-Szenario), bei denen eine private Finanzierung erfolgt, muss sichergestellt werden, dass Kinder aus einkommensschwachen Familien ebenfalls mit Geräten versorgt werden können.
- Bilden Sie ausreichend Rücklagen, um defekte Geräte tauschen und die vorhandene Ausstattung regelmäßig ersetzen zu können (Stichwort „Produktlebensdauer“).

Registrierung bei Dienstleistern (teilweise optional)

- Gerätehersteller
- App-Store
- MDM-Anbieter
- Content-Anbieter

Beschaffung der Geräte

- Fragen Sie vor dem Kauf bei Ihrem Dienstleister, ob und wie Geräte zentral registriert werden können. Dies erspart Ihnen viel Arbeit.
- Die Bestellung von iPads muss bei einem lizenzierten Apple Händler erfolgen, mit dem Hinweis die Geräte gleich für das DEP der Schule zu registrieren. Dazu ist bereits eine DEP-Nummer der Schule nötig (siehe Kapitel 4).
- Sollten bereits iPads an der Schule vorhanden sein, so besteht auch die Möglichkeit diese über den Apple Configurator 2 nachträglich im DEP zu registrieren. (Vgl. <https://support.apple.com/de-de/guide/apple-configurator-2/cad99bc2a859/mac>)
- Samsung-Geräte sollten im Rahmen von Samsung KNOX ebenfalls beim Kauf auf die Schule registriert werden.
- Beim Kauf von Geräten anderer Hersteller sollte überprüft werden, ob/wie diese Geräte registriert und zentral verwaltet werden können.

Rechtliche Rahmenbedingungen (vgl. Kapitel 3)¹

- Einverständniserklärungen der Erziehungsberechtigten
- Nutzungsordnungen und -verträge
- Verträge zur Auftragsdatenverarbeitung (mit Dienstleistern wie, MDM-Anbietern oder App-Herstellern)
- Einhaltung von Datenschutzbestimmungen
- Verfahrensverzeichnisse (Verzeichnis der Verarbeitungstätigkeiten)
- Einhalten von Jugendschutzbestimmungen
- Als lokalen Ansprechpartner können Sie sich zunächst an Ihren Datenschutzbeauftragten wenden.

Versicherung (Diebstahl, Beschädigung, ...)

- Die Privathaftpflicht haftet in der Regel nicht, wenn Geräte verliehen werden!
- Wie ist die Haftung bei BYOD-Szenarien im Unterricht?

Frühe Einbeziehung von Lehrer-, Schüler- und Elterngremien

- Gemeinsame Planung erhöht die Akzeptanz
- Probleme/Widerstände rechtzeitig erkennen und Lösungen finden

1.1.2 Nutzungskonzepte

Nutzungskonzepte wirken sich auf Nutzungsordnungen aus. Wenn sich Einsatzszenarien innerhalb der Schule ändern, sollten Sie darauf achten, dass ggf. Verträge angepasst werden müssen.

Einsatzszenarien für den Geräteeinsatz

- 1:1-Zuordnung: Geräte in der Hand einzelner Benutzer (z.B. Lehrergeräte, Tablet-Klassen, ...)
- 1:N-Zuordnung: Geräte werden von mehreren Anwendern geteilt (z.B. Tablet-Koffer)
- Bring-Your-Own-Device-Konzepte (BYOD)

Soll ein Gerät auch außerhalb der Schule (zu Hause) genutzt werden?

- Darf das Gerät das heimische WLAN/Internet nutzen?
- Darf das Gerät auch zu privaten Zwecken genutzt werden?
- Dürfen andere Familienmitglieder das Gerät benutzen?
- Wer haftet bei Diebstahl/Beschädigung?

¹ S.a. https://lehrerfortbildung-bw.de/st_recht/ und <https://it.kultus-bw.de/Lde/Startseite/IT-Sicherheit/Datenschutz+an+Schulen> und <https://it.kultus-bw.de/Lde/Startseite/IT-Sicherheit/mobile>

- Sollen Geräte offline genutzt werden? Wenn ja, funktionieren alle erforderlichen Apps auch ohne Internet?

1.1.3 Technischer Rahmen

Netzwerkkonzept

- WLAN
- Internetanbindung
- Strukturierte Verkabelung
- Konfiguration der Firewall
- Jugendschutzfilter
- optional: Anbindung der Geräte an die paedML

(technische) Betreuung der Geräte

- Hosting und Pflege MDM-Server (Updates, Backup, ...)
- Alternative zum MDM-Server (z.B. Configurator für iPads)
- Caching-Server
- Einrichtung des Systems
- Fortlaufende Pflege:
 - Verwaltung von Systembenutzern (Administratoren/technische Benutzer/personalisierte Benutzerkonten im MDM (1:1-Szenarien))
 - Konfiguration
 - Gerätesteuerung
 - Geräte zurücksetzen
 - App-Verwaltung
 - Updates einspielen

1.1.4 Pädagogischer Rahmen

Konzepte für den Unterrichtseinsatz

- Wie werden die Geräte im Unterricht eingesetzt?
- Mit welcher Software soll gearbeitet werden?
- Soll von den Geräten präsentiert werden?
- Soll gedruckt werden?
- Welche technischen Kontroll- und Steuerungsmöglichkeiten gibt es? (Classroom-App)

Im Oktober 2018 wurde am Landesinstitut für Schulentwicklung die Handreichung „Im digitalen Zeitalter qualitätsorientiert lernen. Chancen und Grenzen digitaler Medien“ veröffentlicht. Die Handreichung, die sich an Lehrkräfte aller Fächer aus allen Schularten, -stufen und -typen richtet, befasst sich mit den lernförderlichen Potenzialen digitaler Medien. Sie können das Dokument unter <http://www.schule-bw.de/themen-und-impulse/uebergreifende-erziehung/medienerziehung/handreichungen/basisband> herunterladen.

Fortbildung des Kollegiums

- Die Bedienung der Geräte bzw. der eingesetzten Software muss erlernt werden – nicht nur von Schülern sondern gerade auch von den Unterrichtenden! Verschiedene Fortbildner sind denkbar:
 - Lehrer als Multiplikatoren
 - Landeslehrerfortbildung
 - Kreismedienzentrum
 - Dienstleister
 - Arbeitskreise
 - Schulen aus der Region
- Zu rechtlichen Fragestellungen, wie z.B. den Themen Datenschutz und Urheberrecht finden regelmäßig Fortbildungen bei der Landesakademie für Lehrerfortbildung statt

1.2 Anfallende Aufgaben

Die folgende Abbildung veranschaulicht, welche Aufgaben erfüllt werden müssen, damit eine Schule mit Tablets arbeiten kann.

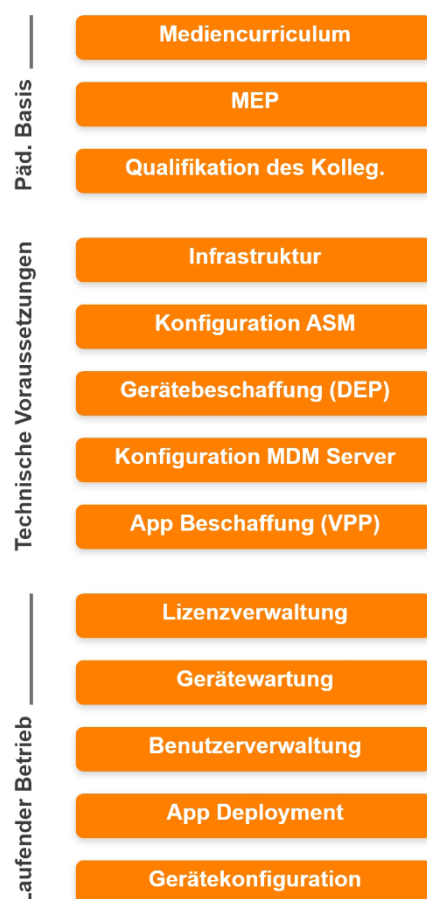


Abbildung: Aufgaben bei der Tablet-Verwaltung bei iOS

Zunächst muss eine „pädagogische Basis“ hergestellt werden. Hierzu gehört die Erstellung eines Mediencurriculums. Im Medienentwicklungsplan (MEP) werden Medienbildungskonzept, Ausstattungskonzept und Fortbildungskonzept erarbeitet.

Hierbei wird auch die Verantwortlichkeit für die technische Betreuung geklärt. Damit im Unterricht gearbeitet werden kann, bedarf es eines qualifizierten Kollegiums.

Unter den „*technischen Voraussetzungen*“ verstehen wir die lokalen Gegebenheiten. Dies sind infrastrukturelle Anforderungen (Netzwerk, Ladestationen, Vorkehrungen für das Geräte-Deployment), ein MDM-Server für die Geräteverwaltung und der Zugriff auf Benutzerkonten, über die Geräte sowie Softwarelizenzen bei den Dienstleistern beschafft und verwaltet werden können.

Unter „*laufender Betrieb*“ schließlich finden sich alle Aufgaben, die sicher stellen, dass Tablets an der Schule konfiguriert und verwendet werden. Hierzu gehören beispielsweise die Zuweisung von App-Lizenzen oder die Benutzerverwaltung.

1.3 Tablets im Schulalltag: Das sollten Sie unbedingt beachten!

- Wie unter <https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/mobile> beschrieben, dürfen auf Geräten, bei der Weitergabe an andere Benutzer, keine Anwendungs-Daten vorheriger Benutzer vorhanden sein. Da weder iOS noch Android systemseitig Daten-Löschmechanismen implementiert haben, müssen die Geräte hierfür komplett zurückgesetzt werden. Dabei gehen auch alle Konfigurationen (Apps, WLAN-Einstellungen, ...) verloren. Hierdurch entsteht ein hoher Betreuungsaufwand. In der Zeit, in der die Geräte zurückgesetzt werden, kann kein Unterricht mit den Geräten stattfinden. Der Umstand, dass Geräte komplett zurückgesetzt werden müssen und keine Daten aus den Apps gelöscht werden können, hat technisch seinen Ursprung im sogenannten Sandbox-Verfahren (vgl. <https://de.wikipedia.org/wiki/Sandbox>). Die Apps laufen hierbei abgeschirmt vom Betriebssystem. Ein Zugriff von Apps auf das OS ist aus Sicherheitsgründen unterbunden. Im Gegenzug kann auch das Betriebssystem nicht auf die Sandboxes zugreifen, um dort z.B. Nutzdaten zu löschen. Folglich müssen die Geräte komplett zurückgesetzt werden.
- Uns ist kein einfach umsetzbares Verfahren für die Protokollierung der Benutzerzugriffe bekannt. Aktuell muss daher die Protokollierung von Benutzerzugriffen über eine händisch zu führende Geräteliste vorgenommen werden. Die Geräte sind für den persönlichen Einsatz konzipiert, eine Authentifizierung gegenüber einer Domäne (wie zum Beispiel einer paedML) ist herstellerseitig nicht vorgesehen. Die Anmeldung an einem WLAN wird von den Geräten dauerhaft gespeichert und kann daher nicht zur Authentifizierung der Benutzer herangezogen werden.

Anmerkung: Die App „filebrowser for education“ (Dateimanager) bietet die Möglichkeit den iPads einen Netzwerkpfad mit zu geben (zum Tauschverzeichnis). Der Schüler meldet sich dann hierbei mit den Logindaten der Netzwerklösung (paedML) an und kann Dateien zwischen iPad und Tauschverzeichnis austauschen.

2. Technische Rahmenbedingungen

2.1 Vergleich der Betriebssysteme iOS und Android

Android und iOS haben sich als Tablet-Betriebssysteme auf dem Markt durchgesetzt und werden in der Schule eingesetzt. Im Folgenden sind Punkte zusammengetragen, die Ihnen bei der Geräteauswahl helfen sollen.

2.1.1 iOS (Apple)

Im direkten Vergleich der Betriebssysteme iOS und Android sehen wir einige Punkte, die für den Einsatz von iOS an Schulen sprechen:

- Zentrale Verwaltung von Geräten über DEP
- Zentrale Verwaltung von (Volumen-)Lizenzen über VPP
- Apps werden direkt an Geräte und nicht an Benutzerkonten verteilt
- Starkes Engagement von Apple auf dem Bildungsmarkt
- Großes Angebot an Apps für den Bildungsbereich
- Geräte haben einen (relativ) langen Produktlebenszyklus und werden vom Hersteller nach Markteinführung ca. fünf Jahre mit Updates versehen
- Mehrere Gerätegenerationen können – durch die gleiche iOS-Version – einheitlich verwaltet werden.
- Geräte können mit anonymen (Geräte-)Konten betrieben werden
- Kostenlose Fortbildungsmöglichkeiten von Apple (vgl. <https://support.apple.com/de-de/HT206841>)
- Fortbildungen durch zertifizierte Apple Trainer (Rabatte ab einer Anschaffung von 25 (halber Schultag zum halben Preis) bzw. 50 iPads (ganzer Schultag zum halben Preis))
- Bildungsrabatt bei Anschaffung von iPads (über Education-Partner)
- Office Apps (Numbers, Keynote, Pages) bereits vorinstalliert und kostenlos nutzbar

Kritik

Apples geschlossenes Ökosystem bietet zwar gut aufeinander abgestimmte Module, andererseits achtet der Hersteller nicht auf verbreitete Standards und zwingt Kunden dazu weitere Peripheriegeräte (z.B. Apple-TV zur Präsentation) zu erwerben. Verschiedene Dongles von Drittanbietern sind deutlich preiswerter und bieten auch die Möglichkeit iOS/Android zu spiegeln, allerdings funktionieren diese nicht immer zuverlässig.

Die Geräte sind relativ teuer. Der Aufwand bei der Geräteverwaltung sollte aber zu den Investitionskosten hinzugerechnet werden, sodass sich hohe Investitionskosten auf Dauer relativieren dürften, da die Verwaltung über ein MDM-System zuverlässig umsetzbar ist.

iPads sind nicht für Mehrbenutzereinsatz gedacht. Datensicherung und Datensicherheit gestalten sich im Alltag als Herausforderung bei einer 1:N-Lösung.

2.1.2 Android (Google)

Im Moment gibt es nach unserer Ansicht Gründe, warum Android Geräte nur eingeschränkt für den schulischen Einsatz geeignet sind:

- Heterogenität der Hardware
- Im Gegensatz zu iOS sind die Einstellungsmöglichkeiten weniger umfangreich – abhängig vom Gerätehersteller und -typ
- Keine verlässlichen Updatezyklen der Hersteller: Bei Android-Geräten werden Updates unregelmäßig veröffentlicht. Upgrades auf neue Android-Versionen sind für viele Geräte nicht verfügbar
- Verfügbarkeit der Geräte – kurze Innovationszyklen führen dazu, dass Geräte nach kurzer Zeit nicht mehr hergestellt werden und vom Markt verschwinden. Eine Beschaffung weiterer baugleicher Geräte wird dadurch mit der Zeit erschwert
- App-Lizenzen werden an Benutzerkonten gebunden, die von der Schule verwaltet werden müssen – es gibt keine Volumenlizenzen, die geräteunabhängig verteilt werden können. Jedes Gerät benötigt daher ein eigenes Google-Konto
- Apps und/oder App-Updates müssen bei MDM-Systemen manuell eingespielt werden, sofern keine zuverlässige Anbindung an den „*Managed Play-Store*“ gegeben ist.
- Geringeres Angebot an hochwertigen Apps für den Bildungsbereich als bei iOS



Der Android-Markt ist gerade in Bewegung und Google erhöht sein Engagement im Wettbewerb um Business-Kunden. Hiervon werden vermutlich auch Schulen profitieren können.

In Kapitel 4.3 ab Seite 29 beschreiben wir, aktuelle Änderungen bei Android.

2.2 Verwaltung

Einzelne Geräte der Schule (z.B. ein Tablet einer Fachschaft) können manuell verwaltet werden – so sich jemand findet, der dies übernimmt.

Ab einer bestimmten Anzahl von Geräten stellt sich die Frage nach einer effizienten Verwaltung. Eine besondere Relevanz erhält die Frage, wenn die Geräte öfter zurückgesetzt werden, häufig Änderungen an der Konfiguration vorgenommen werden sollen oder alle Geräte die gleiche Konfiguration erhalten sollen.

Ein einfaches Verwaltungswerkzeug für iPads bietet Apple mit dem Programm „*Configurator*“, das über einen Mac (Mac mini oder MacBook oder iMac) bedient wird. Die Verwaltung von iPads setzt jedoch voraus, dass die Geräte physikalisch mit dem Mac verbunden werden.

Die Verwaltung mehrerer Endgeräte wird durch ein Mobile Device Management (MDM) vereinfacht. Eine zentrale Instanz ermöglicht Tablets mit einer einheitlichen Konfiguration zu versehen, Benutzer zuzuweisen, Apps zu installieren und Updates zu verwalten.

Ein MDM und/oder der *Configurator* bieten somit die Möglichkeit eine verlässliche Unterrichtsumgebung einzurichten und zu pflegen.

2.2.1 Vorteile eines MDM-Systems

- Konfiguration von Geräten kann zentral geschehen
- es muss keine (physikalische) Verbindung zu den Endgeräten bestehen, um Änderungen auszuspielen.
- mehrere Geräte können mit der gleichen Konfiguration bespielt werden
- das Auf-, und Zurücksetzen kann (weitgehend) automatisiert werden
- Konfiguration der „Classroom App“ nur über MDM System möglich.

2.2.2 Auswahl und Einrichtung eines MDM-Systems

Das Landesmedienzentrum kann aktuell keine Produktempfehlung für ein MDM-System geben. Erkundigen Sie sich in Ihrer Region, zum Beispiel in Ihrem Kreismedienzentrum oder bei Ihrem Schulträger, ob es Möglichkeiten gibt die Geräteverwaltung von Schulgeräten über ein zentrales MDM-System eines regionalen IT-Dienstleisters abzubilden.

Für die Installation des MDM-Servers bieten sich mehrere Möglichkeiten:

1. externes Hosting

Über ein externes (zentrales) Hosting können mehrere Systeme über einen Server abgebildet werden. Ihre Schule erhält einen Zugang zu einem eigenen Bereich („Mandant“), über den die Verwaltung des eigenen MDMs geschieht.

Ein entscheidender Vorteil dieses Verfahrens ist die Entlastung der Schule von der Einrichtung und der Administration des MDM-Servers. Bei der Auswahl eines zentralisierten Servers sollten Konzepte wie die hohe Verfügbarkeit der Server, Backupkonzepte und die Serverwartung vom Serviceanbieter angeboten werden.

Viele Hersteller bieten Ihre Produkte als „Software-as-a-Service“ an. Hierbei fallen bei manchen MDM-Lösungen keine weiteren Kosten an, da das Hosting in den Lizenzgebühren enthalten ist. Manche Anbieter verlangen Gebühren für Schulungen, die Systemeinrichtung und Wartungsverträge, die im Support-Fall notwendig werden.

2. eigenes Hosting

Alternativ kann ein MDM-System auch in der IT-Infrastruktur der Schule/des Schulträgers installiert werden. Dies bedeutet in der Summe jedoch einen erhöhten Kosten- und Personalaufwand (Beschaffung, Einrichtung und Betreuung des MDM-Servers, Einspielen von Updates, Erstellen von Backups, ...) und bietet selten einen Mehrwert gegenüber einem externen Hosting.

2.2.3 Einsatzszenarien für den Geräteinsatz

Durch unterschiedliche Konfigurationen können verschiedene Anwendungsszenarien erarbeitet und an die Geräte ausgespielt werden. So erhalten Lehrergeräte, die dauerhaft bei den Pädagogen verbleiben, eine andere Konfiguration als Geräte, die im Unterricht von verschiedenen Schülern genutzt werden.

1:1-Szenario

Tablets können in einem 1:1-Szenario, bei dem ein Nutzer dauerhaft dasselbe Endgerät bedient, konkreten Personen zugewiesen werden. Für ein solches Einsatz-Szenario gilt es rechtliche Fragen zu beachten und zum Beispiel in Nutzungsordnungen abzubilden. Bei der Nutzung von kommerziellen Cloud-Angeboten ist grundsätzlich zu prüfen, dass die Angebote datenschutzrechtlich unbedenklich sind und ein Auftrag zur Datenverarbeitung mit dem jeweiligen Anbieter abzuschließen.

Bei der Nutzung eines 1:1-Szenarios hat jeder Benutzer Zugriff auf seine eigenen Dateien, die lokal auf dem Gerät gespeichert werden. Die Endgeräte können für die Nutzer dauerhaft zur Ablage von Daten in definierten Datenspeicher (z.B. im pädagogischen Netz) eingerichtet werden.

Bei 1:1-Szenarien ist dringend zu klären, ob und wie die Geräte auch privat genutzt werden können. Dies ist sowohl vertraglich als auch in der Konfiguration der Geräte abzubilden, sofern diese außerhalb des Schul-Campus andere Einstellungen erhalten sollen.

Beispiele für 1:1-Szenarien ist die Vergabe von personalisierten Tablets an das Kollegium oder der Einsatz von Geräten in einer Tablet-Klasse, z.B. innerhalb einer Berufsschule.

1:N-Szenario

In 1:N-Szenarien nutzen mehrere Anwender ein Gerät. Für diesen Fall empfiehlt es sich, **technische Benutzer** an die Geräte zuzuweisen. Die Geräte können zum Beispiel Tablet 1 bis Tablet N genannt werden und die gleichen Bezeichnungen werden als Benutzernamen an die Geräte zugewiesen.

Geräte, die als Lehrergeräte genutzt werden sollen, können hierbei eine eigene Konfiguration (z.B. weitere Apps, Lehrergerät für Apples „Classroom“-App, ...) erhalten.

Ein Mehrbenutzer-Szenario, eine Anmeldung an einer Domäne, der Zugriff auf eine zentrale Dateiablage (zum Beispiel in der paedML) sind herstellerseitig zunächst nicht vorgesehen. Bei 1:N-Szenarien entstehen daher besondere Herausforderungen:

- Bei 1:N-Szenarien findet aktuell keine Protokollierung des Nutzerzugriffs statt. Daher wird empfohlen, dass über händisch gepflegte Benutzerlisten protokolliert wird, welche Geräte wann an SchülerInnen ausgegeben werden.
- Bei 1:N-Szenarien müssen die Geräte zurückgesetzt werden, um zu verhindern, dass persönliche Daten von anderen Nutzern eingesehen werden.
- Beim Zurücksetzen werden alle Daten von den Geräten gelöscht. Daher muss überlegt werden, wie Daten für eine spätere Bearbeitung gespeichert werden können (Export auf Netzlaufwerke oder in eine Private Cloud). Es ist nicht möglich alle Daten zu speichern. Projektdateien (zum Beispiel aus Videobearbeitungsprogrammen) können häufig nicht exportiert werden. In solchen Fällen dürfen die Geräte nicht zurückgesetzt werden, bis ein Video-Projekt abgeschlossen ist!

Shared iPads

Mit dem Konzept "Shared iPads" ermöglicht Apple seit 2016 eine Multiuserfähigkeit von iPads. Hierbei werden für die Anwender der Schule Benutzerkonten bei Apple angelegt.

Ein Schüler meldet sich mit seinem Benutzerkonto auf einem iPad an und kann dann auf seine persönlichen Daten zugreifen. Auf Daten von anderen Anwendern, die mit dem gleichen Gerät gearbeitet haben, kann nicht zugegriffen werden. Die Daten werden in der

iCloud gespeichert und bei Bedarf aus der Cloud heruntergeladen – zum Beispiel, wenn ein Benutzer noch nicht auf dem jeweiligen Gerät angemeldet war.



Shared iPads dürfen aktuell in Baden-Württemberg aus Datenschutzgründen nicht genutzt werden, da personenbezogene Daten in die Cloud übertragen werden.

Es reicht nicht, die Benutzer zu anonymisieren, da nicht sichergestellt werden kann, welche Daten in die Cloud geladen werden. Fotos von Schülern zum Beispiel dürfen nicht ohne vorherige Zustimmung (durch die Betroffenen und deren Erziehungsberechtigten) in die Cloud übertragen werden. Die Ablage personenbezogener Daten in der Cloud ist ebenfalls strengstens zu regulieren – im Idealfall völlig zu unterbinden. Insbesondere Leistungsbewertungen, die z.B. auf Lehrer-Tablets erhoben werden, dürfen nicht in die Cloud übertragen werden!

In dem Dokument „Apple im Bildungsbereich Überblick Datenschutz und Privatsphäre für Schulen“ vom April 2018 (aufgerufen im Februar 2019), steht explizit, dass Daten auch außerhalb der EU und damit außerhalb des Wirkungsbereiches europäischer Datenschutzbestimmungen gespeichert werden können.

Internationaler Datentransfer

(...)

Mit Apple School Manager, verwalteten Apple-IDs und iCloud können persönliche Daten in einem anderen Land als dem Ursprungsland gespeichert werden. Unabhängig davon, wo die Daten gespeichert werden, unterliegen sie 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, vom von der Europäischen Kommission genehmigtem Model Contractual Clauses/Swiss Transborder Data Flow Agreement geregelt werden– oder durch ein operatives Privacy Shield Zertifizierungsprogramm, für das Apple Inc. vielleicht zertifiziert wird. Die Model Contractual Clauses und das Swiss Transborder Data Flow Agreement sind dem Apple School Manager Vertrag angehängt.

Quelle: „Apple im Bildungsbereich Überblick Datenschutz und Privatsphäre für Schulen“, S. 7, Fehler im Original

(https://www.apple.com/de/education/docs/Data_and_Privacy_Overview_for_Schools.pdf)

Bring Your Own Device

Bei „Bring Your Own Device“ (BYOD) werden private Geräte im Unterricht eingesetzt.

Die Verwaltung privater Endgeräte durch die Schule birgt Risiken.

BYOD mit MDM

Eine (Teil-)Verwaltung privater Endgeräte kann über ein schulisches MDM abgebildet werden. Geräte werden hierfür in das MDM aufgenommen und können dadurch mit Apps oder speziellen Konfigurationen versehen werden. In diesem Fall ist es i.d.R. möglich, dass Anwender die Verwaltung aufheben, indem sie das MDM-Profil von den Geräten entfernen.

Alternativ können auch Apps über das MDM an eine private Apple ID verteilt werden, so dass eine Einbindung des privaten Geräts in das MDM nicht notwendig ist. Die schulischen Apps findet der User dann in seinen "Einkäufen" wieder, wo Sie auch noch 30 Tage nach Entzug der App zur Verfügung stehen.

Mögliche Probleme bei BYOD-Szenarien sind:

- Haftungsfragen, z.B. beim Datenverlust durch das Zurücksetzen von Endgeräten
- Erhöhter Aufwand bei der Geräteadministration – sofern über ein MDM verwaltet.
- Eine heterogene Hardware-Ausstattung bei den Schülern stellt besondere Anforderungen an den Administrator, der verschiedene Geräteklassen, Betriebssysteme und Betriebssystem-Versionen verwalten muss.
- Wie geht man mit Nutzern um, die ihr Gerät nicht durch die Schule verwalten lassen wollen?

BYOD generell

Wenn ein BYOD-Ansatz (auch ohne MDM) umgesetzt wird, müssen die folgenden Punkte bedacht werden:

- Sicherheitsaspekte:
 - Auswirkungen nicht von der Schule verwalteter Geräte mit administrativen Rechten im Schulnetz (z.B. Anwender bringen Software, die für Angriffe innerhalb des Schulnetzes genutzt werden kann).
 - Es besteht die Gefahr, dass Viren/Malware durch nicht geschützte Geräte verteilt werden.
- Eine Trennung der schulischen Netze von Netzen mit BYOD-Nutzung wird dringend empfohlen.
- Uneinheitliche App-Versionen und heterogene Betriebssysteme der Schülergeräte können im Unterricht zu Problemen führen, sofern eine bestimmte App benötigt, die nicht auf allen Schülergeräten vorhanden ist.
- Die Anforderungen an das Schulnetz steigen immens, wenn viele Benutzer gleichzeitig auf das Netz zugreifen. So sollten in diesem Fall Updates der Geräte unterbunden werden und ein sinnvolles Bandbreitenmanagement zum Einsatz kommen.
- Ein leistungsstarkes Netz (WLAN und Internetanbindung) ist zwingend notwendig.
- Die Ungleichheit der Ausstattung mit Endgeräten kann zu einem sozialen Druck unter Schülern führen.
- Wie geht man mit Nutzern um, die kein mobiles Endgerät besitzen?
- Haftungsfragen, wenn private Geräte im Unterricht genutzt werden – ist die Schule versichert?

- Wie werden Nutzerzugriffe protokolliert? (Der Einsatz eines Radius-Servers mit Benutzer-Authentifizierung ist zum Beispiel ein Lösungsansatz.)
- Wie werden Datenschutzerfordernungen umgesetzt?
- Gibt es einen Jugendschutzfilter?
- Gibt es eine spezielle Nutzungsordnung von schulischer Netzwerkinfrastruktur durch private Geräte?

Abgesehen von den hier aufgeführten Punkten könnte ein BYOD-Ansatz niederschwellig umgesetzt werden, wenn es beispielsweise „nur“ darum geht im Internet zu recherchieren, da die Geräte der Schüler häufig über internetfähige Endgeräte und entsprechende Verträge verfügen.

Der Ausbau und die Bereitstellung einer WLAN-Infrastruktur für alle am Schulleben Beteiligte könnte ebenfalls ein BYOD-Ansatz sein, wobei ein leistungsfähiges WLAN, für den Schulcampus, kostenintensiv

2.2.4 Geräte-Konfiguration

Voraussetzung für eine (einheitliche) Konfiguration der Geräte ist, dass diese über das MDM betreut werden.

Die Konfigurationsparameter sind abhängig vom eingesetzten Betriebssystem und der jeweiligen Version. Mit steigenden Versionsnummern werden neue Funktionen eingeführt und alte Funktionen teilweise deaktiviert.



Es ist dringend notwendig regelmäßig zu überprüfen, ob die Konfigurationsparameter noch aktuell sind und Anpassungen an der Konfiguration notwendig sind!

Über die Gerätekonfiguration werden verschiedene Aufgaben umgesetzt.

- technische Einbindung der Geräte in das Schulnetz
- Umsetzung des Einsatzszenarios
- Festlegen von Funktionen und Restriktionen (Was dürfen Anwender mit den Geräten machen?)

Die Definition der Konfigurationsparameter ist eine wichtige Aufgabe bei der Einführung von Tablets an der Schule. Die Konfiguration der Tablets ist abhängig von verschiedenen Faktoren und muss individuell in der Schule erarbeitet werden.

(technische) Einbindung der Geräte in das Schulnetz

- Netzwerkkonfiguration (WLAN, Proxy-Server, Filter , ...)
- *optional*: Konfiguration von Programmen (z.B. für die Anbindung von Netzlaufwerken)
- *optional*: Übergabe von Zertifikaten (z.B. für Anmeldung an Firewall)
- *optional*: Einrichtung von Mailservern oder Kalendern (z.B. für Nutzung von Mailserver durch Lehrer-Geräte)

Einsatzszenario:

- Werden die Geräte von nur einem Benutzer verwendet?
- Werden die Geräte von mehreren Benutzern verwendet?
- Restriktionen bei Lehrergeräten werden vermutlich weniger streng definiert als bei der Nutzung durch Schüler
- Dürfen Geräte auch privat genutzt werden?
- Dürfen Benutzer bei der privaten Geräte-Nutzung kommerzielle Cloud-Services nutzen?

Funktionen und Restriktionen

- Darf auf die Kamera zugegriffen werden?
- Soll Bluetooth genutzt werden (Classroom-App, Datenaustausch zwischen Geräten, ...)?
- Werden die Geräte auch außerhalb der Schule verwendet (und müssen Nutzer dabei das WLAN ändern können)?
- Umsetzung von Datenschutzrichtlinien (z.B. über das Deaktivieren von Cloud-Diensten)
- Beschränkung auf einzelne Apps (Kioskmodus)?
- Gerätelayout (Gruppierung von Apps, Hintergrund, Nachrichten auf Sperrbildschirm, ...)
- ...

2.2.5 App-Installation

Die App-Installation kann benutzer- oder gruppenspezifisch erfolgen. So können Lehrer andere Apps erhalten als Schüler, Geräte, die für Fachschaften konzipiert werden, können ebenfalls spezielle Apps erhalten.

Besonders interessant ist dies, wenn Lizenzen für kostenpflichtige Apps verteilt werden. Sie können diese dynamisch an einzelne Geräte zuweisen und bei Bedarf die Lizenz wieder entziehen, um sie an andere Benutzer/Geräte zu übergeben.

Anmerkung: Je nach Anbieter verfügt das MDM ggf. auch über eine hauseigene App, über die Apps bereitgestellt und bei Bedarf heruntergeladen werden können. Dies bietet den Vorteil, dass beim Zurücksetzen der iPads nicht alle Apps automatisch gepusht werden und dadurch die Netzauslastung geringgehalten wird (interessant bei 1:n Szenario und der Nutzung großer Apps (z.B. Garageband)).

2.3 Netzwerk



Der folgende Abschnitt beinhaltet Punkte, die nicht in jeder Schule sinnvoll sind. Eine Grundschule mit fünf iPads benötigt sicherlich keinen Serverraum mit Glasfaseranbindung in jedes Klassenzimmer. Die Erfahrung zeigt jedoch, dass unzureichende Netzwerkinfrastrukturen häufige Fehlerquellen sind, die durch gute Planung vermieden werden können.

Ohne zuverlässige strukturierte Verkabelung ergibt der Einsatz von IT an der Schule in der Regel wenig Sinn. Der Betrieb von mobilen Endgeräten wie Laptops, Tablets, etc. stellt besondere Anforderungen an die schulische IT. Je mehr Geräte über WLAN an das Schulnetz angeschlossen werden, desto leistungsfähiger muss das WLAN sein –

Consumer-Hardware (z.B. ein beim Mediendiscountern beschaffter Accesspoint, PowerLan -Adapter, ...) kommt dabei in der Regel schnell an ihre Leistungsgrenze.

2.3.1 Internetanbindung

Die Internetanbindung sollte abhängig von verschiedenen Faktoren umgesetzt werden:

- Werden große Datenmengen (zeitgleich) aus dem Internet geladen (z.B. gleichzeitiges Zurücksetzen von 30 Tablets (vgl. hierzu Kapitel 2.5, S. 20)?
- Wie viele Anwender greifen zeitgleich auf das Internet zu (und was machen sie dabei)?
- Wie groß muss der Upstream bemessen sein? Werden auch Daten in eine externe (private) Cloud hochgeladen (z.B. Cloudspeicher bei einem Dienstleister)?

2.3.2 WLAN und Netzwerkinfrastruktur

Das WLAN muss ebenfalls an die Anzahl der Endgeräte angepasst werden. Stichworte zum WLAN an der Schule:

- **Strukturierte Verkabelung nach EN 50173-1 (2003)**
 - Empfehlung: durchgängig 1 Gigabit-Verkabelung bis zu den Clients (Stand 2018)
 - keine WLAN-Repeater / keine Meshing-Technologie
 - keine Powerline-Adapter
- **Fast-Roaming** (s.a. https://en.wikipedia.org/wiki/IEEE_802.11r-2008) – Die Anwender bewegen sich im Schulgebäude - die Accesspoints sollten in der Lage sein diese Bewegungen abzubilden.
- **Lastausgleich** – hiermit kann ein WLAN Verbindungen von mobilen Endgeräten auf verschiedene Accesspoints verteilen, um das Netzwerk und Funkspektrum optimal auszunutzen und zu verhindern, dass sich Geräte nur auf einem AP einwählen, während der direkt daneben befindliche AP nicht benutzt wird.
- **Client-Isolation** – Während es in einem "normalen" WLAN in der Schule Sinn ergeben kann, dass mobile Endgeräte voneinander getrennt werden, um z.B. um Filesharing zu unterbinden, steht diese Technologie diversen Einsatzszenarien von Tablets im Unterricht im Weg, da es hier durchaus erwünscht sein kann, dass die mobilen Endgeräte miteinander kommunizieren. Ggf. ist hier ein eigenes Tablet-Netz vorzusehen. **Anmerkung:** Voraussetzung für die Verwendung der „Classroom App“.
- **Multi-SSID** – Ein Accesspoint kann mehrere Netze mit unterschiedlichen SSIDs bereitstellen und unterschiedlichen VLANs zuordnen.
- **VLAN** – Die aktive Netzinfrastruktur sollte in der Lage sein, virtuelle Netze zu verwalten. Dies verhindert, dass Sie für jedes Netzwerk exklusive End- und Vermittlungsgeräte (inklusive Verkabelung, ...) betreiben müssen (große Kostenersparnis).
- **Management** – WLAN-Geräte, die über eine zentrale Administrationskonsole verwaltbar sind, bedeuten weniger administrativen Aufwand. Anstatt eine Konfigurationsänderung in jedem Gerät einzeln vornehmen zu müssen, können Sie diese bei gemanagten Systemen zentral einspielen und verteilen.

2.3.3 Jugendschutzfilter

Ein Internetzugang ohne Jugendschutzfilter ist äußerst problematisch. Im pädagogischen Netz der paedML werden jugendgefährdende Internetinhalte gefiltert. Wenn Sie keine paedML einsetzen sollten Sie Sorge dafür tragen, dass ein Jugendschutzfilter eingerichtet ist.



Wir empfehlen baden-württembergischen Schulen den Internetzugang über BelWü umzusetzen. BelWü bietet verschiedene Pakete an (vgl. <https://www.belwue.de/produkte/preise.html>). Ein Jugendschutzfilter ist über den im Internetzugang enthaltenen BelWü-Proxy-Server verfügbar.

2.4 Aufbewahrung der Geräte

Mobile Endgeräte sind in der Regel nicht ständig mit einem Stromkabel verbunden. Um sicherzustellen, dass die Geräte im Unterricht genutzt werden können, muss einerseits dafür gesorgt werden, dass die Geräte nach der Benutzung wieder aufgeladen werden. Andererseits muss vorgesorgt werden, falls ein Akku im laufenden Betrieb leer ist. Ausreichend Steckdosen und Ladegeräte sollten daher im Klassenzimmer vorgehalten werden.



Achten Sie auf eine richtige Pflege der Akkus!

Weder die dauerhafte Verbindung mit dem Ladegerät noch die regelmäßige Tiefenentladung sind förderlich für die „Akku-Gesundheit“.

Die Geräte sollten regelmäßig geladen werden, Zeitschaltuhren verhindern eine dauerhafte Überladung.

Die Frage nach der Aufbewahrung wird sinnigerweise auch mit der Frage nach dem Zurücksetzen der Geräte verbunden. Über spezielle Lösungen verschiedener Hersteller können iPads aufbewahrt, geladen und (zeitgleich) zurückgesetzt werden. Hierfür gibt es verschiedene Koffer- oder Schranklösungen, die ähnlich wie ein Laptop-Wagen, genutzt werden können.

Mit der Mobilität der Geräte geht ein höheres Diebstahlrisiko einher. Es sollte also auch sichergestellt werden, dass die Geräte nach der Nutzung weggeschlossen werden, um Diebstahl zu verhindern. Über Sperrfunktionen können Geräte unbrauchbar gemacht werden. Sofern eine Internetverbindung besteht, können entwendete Geräte geortet und im Idealfall wiederbeschafft werden. Für einen potenziellen Dieb sind DEP registrierte Geräte wertlos, da sie nach einem Diebstahl aus der Ferne gelöscht und blockiert werden können. Dieser Schutz ist praktisch nicht zu umgehen!

2.5 Caching-Server

Zur Entlastung der Internetverbindung empfehlen wir den Einsatz eines Caching-Servers, der Apps und Betriebssystem-Updates zentral im Schulnetz zwischenspeichert (vgl. <https://support.apple.com/de-de/guide/mac-help/about-content-caching-mchl9388ba1b/mac>).

2.5.1 iOS-Geräte

Zum Cachen von iOS-Inhalten wird ein Gerät mit Mac-OS (z.B. ein Mac mini) eingesetzt. **Das Gerät muss immer verfügbar sein, wenn die iPads im Betrieb sind.** Das Gerät muss außerdem im selben Netzsegment wie die iPads betrieben werden.

Trotzdem kann es vorkommen, dass die (W)LAN-Performance einbricht, wenn zu viele Geräte gleichzeitig ein Update über das WLAN laden.

Für ein schnelleres Wiederherstellen können iPads über (USB-) Kabel mit dem Caching-Server verbunden werden (z.B. über einen Koffer, der gleichzeitig als Ladestation genutzt wird).

Damit die Tablets mit ausreichend Strom versorgt werden, sollte ein aktiver USB-Hub zum Einsatz kommen, an den die Geräte angeschlossen werden. Kofferlösungen (s. vorheriger Abschnitt „Aufbewahrung der Geräte“) haben einen solchen USB-Hub in der Regel bereits integriert.

Anmerkung: Sollten die Geräte via Apple Configurator ihr WLAN Profil etc. erhalten, ist Voraussetzung, dass der Tablet-Koffer über einen Synchronisationsmodus verfügt.

2.5.2 Android-Geräte

Für Android-Geräte ist uns aktuell kein Caching-Verfahren bekannt.

2.6 Peripherie

2.6.1 Drucken (iOS)

Soll von den Geräten aus gedruckt werden, müssen folgende Bedingungen erfüllt sein:

- Die App muss das Drucken unterstützen.
- Der Drucker muss AirPrint unterstützen (<https://support.apple.com/de-de/HT201311>).
- Der Drucker muss im gleichen Netz verfügbar sein, in dem die iPads betrieben werden.

Die Einrichtung eines AirPrint-Druckers kann über das MDM-System realisiert werden. Hier werden Drucker an die Tablets zugewiesen.

2.6.2 Präsentation

Die Präsentation geschieht meistens drahtlos. Zur Präsentation von Bildschirminhalten wird ein Präsentationsmedium (Beamer, interaktive Tafel, ...) benötigt. Apple setzt für die Präsentation AirPlay-kompatible Hardware (<https://www.apple.com/de/airplay/>) voraus.

Andere Hersteller nutzen Standards wie *Intels Wireless Display-Adapter (WiDi)*, die von vielen handelsüblichen Beamern bereits unterstützt werden oder über WiDi-Adapter nachgerüstet werden können.

Es gibt auf dem sich ständig entwickelnden Markt verschiedene Anbieter, deren Produkte wir hier nicht im Einzelnen bewerten können. Über Ihr regionales Kreismedienzentrum,

Ihren Dienstleister sowie eine Internetrecherche zu diesem Thema können Sie weitere Informationen zu diesem Thema erhalten.

Die Präsentation von Schüler-iPads kann im Unterricht mit der Classroom-App (vgl. https://images.apple.com/chde/education/docs/getting-started-with-classroom-2.0_de-CH.pdf) erfolgen.

Anmerkung: Neue Monitormodelle beinhalten teilweise "AirPlay2", so dass die Anschaffung eines Apple TV etc. überflüssig wird. Die Funktion "AirPlay2" setzt jedoch IOS 11.4 voraus.

2.6.3 Zubehör

Optional kann über die Beschaffung folgenden Zubehörs nachgedacht werden:

- **Schutzhülle** – gibt es in verschiedenen Ausführungen, von schlicht über schick bis hin zu (nahezu) unzerstörbar.
Achtung: Geräte mit geschlossener Schutzhülle schalten das WLAN aus, sodass sie keine Konfigurationsänderungen erhalten, wenn sie im Schrank liegen!
Achtung: Achten Sie vor der Beschaffung von Schutzhüllen darauf, dass weder Kamera noch Mikrofon der Geräte verdeckt werden.
- **Displayschutz** – hilft häufig gegen Kratzer
- **Stifte** (aktiv/passiv) – Nicht jedes Gerät unterstützt jeden Stift
- **Externe Tastaturen** - z.B. zum Erlernen des 10-Finger Systems
- **Apple-TV** – notwendig für die Bildschirmpräsentation
- **AirPrint-fähige Drucker** – wenn direkt von den Endgeräten gedruckt werden soll.
- **Stative** – (z.B. für Trickfilmprojekte, zur Nutzung als Dokumentenkamera, ...)
- **Kopfhörer** – und Splitter, falls die Geräte von mehreren Schülern genutzt werden
- **Lautsprecher** – zum gemeinsamen Anhören von Medien
- **Aufbewahrungs-/Ladestationen** – können auch für das „Ausrollen“ der Geräte genutzt werden. Hier gibt es verschiedene (teilweise sehr teure) Produkte auf dem Markt. Mit ein bisschen Kreativität lassen sich auch im Werkunterricht interessante Lösungen finden.

3. Rechtliche Rahmenbedingungen

Neben technischen sind auch organisatorisch-rechtliche Fragestellungen zu beachten. Hierzu gehören folgende Themen:

- Einverständniserklärungen
- Datenschutz
- Verfahrensverzeichnis / Verzeichnis der Verarbeitungstätigkeiten
- Nutzungsordnungen
- Vertragsverhältnisse zwischen Schule und schulrelevanten Gruppen
- Versicherungen
- Finanzierung

Das Kultusministerium stellt unter <https://it.kultus-bw.de/Lde/Startseite/IT-Sicherheit/mobile> Informationen zum Datenschutz beim Einsatz mobiler Endgeräte bereit. Hier wird in zwei Dokumenten ausgeführt, was beim Einsatz an der Schule beachtet werden muss.

Dokument „Hinweise beim Einsatz von Tablets“

Das Dokument „Hinweise für den Einsatz mobiler Endgeräte im Unterricht“ beschreibt ausführlich, worauf Schulen bei der Einrichtung und dem Betrieb schuleigener Geräte achten sollten in Hinblick auf den Datenschutz: Geklärt werden muss, wie beispielsweise mit personenbezogenen Daten umgegangen wird, welche Daten verarbeitet und wie Daten anonymisiert werden können.

Das Papier beschreibt, wie die Schule mit Bildern und Videos aus Schülerprojekten umgehen kann und welche Einwilligungen im Vorfeld von den Erziehungsberechtigten und von den Schülerinnen und Schülern eingeholt werden müssen.

Das Dokument behandelt weiterhin die Themen „Störerhaftung“ und „Providerhaftung“ aus schulischer Sicht, wie mit strafrechtlich relevanten Inhalten umzugehen ist und wann personenbezogene Schülerdaten verschlüsselt werden müssen. (Begriffserläuterungen siehe Dokument Seite 3)

Dokument „Leitfaden für die Nutzung von Apps“

Der „Leitfaden für die datenschutzkonforme Auswahl und Nutzung von Apps“ behandelt den Umgang mit personenbezogenen Daten auf Tablets oder Handys eingehender. Das Dokument verweist darauf, dass die Schule selbst verantwortlich für den Schutz der Daten ist. Schulen sind dazu verpflichtet, einen Auftragsverarbeitungsvertrag abzuschließen, sobald personenbezogene Daten durch externe Dienstleister verarbeitet werden.

Solche Daten fallen zum Beispiel bei personalisierten Benutzerkonten innerhalb von Cloud-Services aber auch bei der Nutzung von Apps an, sofern diese Apps personalisierte Daten in die Cloud übertragen und außerhalb der schulischen IT-Infrastruktur speichern.

Es ist vor der Nutzung einer jeden App zu überprüfen, ob die rechtlichen und die technischen Voraussetzungen für einen unbedenklichen Betrieb der App gegeben sind. Hierzu gehört zum Beispiel, dass Nutzerdaten nicht an Dritte weitergegeben werden dürfen.

Erst wenn alle in dem Leitfaden aufgeführten Kriterien positiv erfüllt sind, kann eine App als geeignet bewertet werden, andernfalls sollte von einer Nutzung abgesehen werden.

Am Ende des Dokuments werden weitere Tipps für den Betrieb von Geräten an der Schule gegeben.

Auf den Seiten des Lehrerfortbildungsservers finden Sie hilfreiche Informationen zu rechtlichen Fragen beim Datenschutz. Exemplarisch möchten soll an dieser Stelle die Seite https://lehrerfortbildung-bw.de/st_recht/ genannt werden.

3.1 Datenschutz

Unter <https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/index.html> finden Sie anschaulich aufbereitete Informationen zum Thema Datenschutz an Schulen, die vom Schulministerium NRW aufbereitet wurden. **Achtung! Beachten Sie, dass unter Umständen in Baden-Württemberg abweichende Vorschriften gelten!**

Beim Thema Datenschutz geht es generell darum das informationelle Selbstbestimmungsrecht der Anwender zu wahren. Konkret bedeutet das, dass personenbezogene Daten nicht achtlos weitergegeben werden dürfen.

Folgende Punkte gilt es zu beachten²:

- **Vertraulichkeit** – Nur Befugte können personenbezogene Daten zur Kenntnis nehmen.
- **Integrität** – Personenbezogene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell.
- **Verfügbarkeit** – Personenbezogene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß verarbeitet werden.
- **Authentizität** – Personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet werden.
- **Revisionsfähigkeit** – Es kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.
- **Transparenz** – Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten sind vollständig, aktuell und in einer Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen werden können.
- **Datenvermeidung und Datensparsamkeit** – Daten nur wenn wirklich notwendig mit Dritten teilen
- **Zweckbindung** – Unterbinden der Weitergabe von Daten an Dritte, bzw. der Verwendung für andere Zwecke)
- **Erhebungsgrundlage** – Damit Daten erhoben und verarbeitet werden dürfen, bedarf es einer rechtlichen Grundlage oder der Zustimmung der Betroffenen.

Statt personenbezogene Daten an Cloud-Anbieter zu übermitteln, kann die Schule auch mit der Anonymisierung, bzw. der Pseudonymisierung der Benutzerdaten arbeiten. Anonymisierung bedeutet, dass die Daten keinen Personenbezug haben, Pseudonymisierung bedeutet, dass statt des Klarnamens eines Benutzers ein Alias (Schüler135, Biene-Maja23, ...) angelegt wird.

Leider besteht weiterhin das Problem, dass die Daten, die von Anwendern in die Cloud übertragen werden, selbst datenschutzrechtlich relevant sein können. So kann zum Beispiel ein in die Cloud übertragenes Foto die Bildrechte der fotografierten verletzen. **Dies führt dazu, dass Sie genau überprüfen müssen, ob ein externes Angebot (wie ein Cloudspeicher oder eine datensammelnde App) im Unterricht eingesetzt werden darf!**

² Quelle: <http://www.medienberatung.schulministerium.nrw.de/Medienberatung/Publikationen/aktuelle-Publikationen/Datenschutz.html>

3.2 Verfahrensverzeichnisse

Gemäß Datenschutzgesetzgebung muss die Verarbeitung personenbezogener Daten in einem Verfahrensverzeichnis dokumentiert werden. Mit der Umsetzung der EU-Datenschutzgrundverordnung ist hierfür Begriff „Verzeichnis der Verarbeitungstätigkeiten“ eingeführt worden. Darin ist festzuhalten, wie personenbezogene Daten verarbeitet werden (z.B. Speicherort, Löschfristen, wer kann Daten einsehen, ...)

Weitere Infos finden Sie auf den Seiten der Lehrerfortbildung unter https://lehrerfortbildung-bw.de/st_recht/daten/ds_neu/verfahren/.

3.3 Verträge zur Auftragsdatenverarbeitung

Sobald personenbezogene Daten durch Dritte eingesehen und / oder bearbeitet werden (z.B. Fernzugriff durch Dienstleister auf Systeme, in denen personenbezogene Daten verarbeitet werden; Speicherung von Daten bei einem externen Dienstleister (z.B. Cloud-Anbieter); Weitergabe von Daten an App-Anbieter; ...), benötigt die Schule einen Vertrag zur Auftragsdatenverarbeitung mit dem jeweiligen Anbieter. Die Dokumente unter <https://it.kultus-bw.de/Lde/Startseite/IT-Sicherheit/mobile> bieten Hinweise, was bei der Arbeit mit Tablets zu beachten ist.

Unter https://lehrerfortbildung-bw.de/st_recht/daten/ds_neu/auftrag/ finden Sie weitere Informationen zu diesem Thema.

3.4 Nutzungsordnungen

Es wird dringend empfohlen (für die verschiedenen Anwendungsszenarien an Ihrer Schule) Nutzungsordnungen zu erstellen und von den Anwendern unterschreiben zu lassen. Ein Muster finden Sie unter <https://it.kultus-bw.de/Lde/Startseite/IT-Sicherheit/mobile>.

Weitere Informationen und Beispiele finden Sie unter https://lehrerfortbildung-bw.de/st_recht/form/netz/

3.5 Versicherungen

Suchen Sie vor der Anschaffung mobiler Endgeräte gemeinsam mit Ihrem Schulträger nach einer Lösung zum Thema „Versicherung“.

Sofern ein BYOD-Szenario angedacht ist, sollte im Vorfeld geklärt werden, wie private Geräte für die Zeit, in der sie im Unterricht verwendet werden, versichert werden können.

4. Registrierung der Geräte und Lizenzierung von Apps

Die Gerätehersteller und die Softwareanbieter (Apple und Google) bieten verschiedene Angebote, um Endgeräte zu verwalten und Software zu verteilen. Hierfür müssen Sie sich bei den jeweiligen Anbietern registrieren, um ein Benutzerkonto zu erhalten.



Nutzen Sie nach Möglichkeit keine personalisierte Emailadresse für die Registrierung bei Dienstleistern. Funktionsadressen, wie z.B.

Tablets@Meine-Schule.de können weiterverwendet werden, wenn Verantwortliche für die Tablet-Betreuung wechseln.

Im Folgenden werden die Angebote von Apple und Google beschrieben.

4.1 iOS (Apple)

4.1.1 Apple School Manager (ASM)

Unter school.apple.com können sich Bildungseinrichtungen im Apple-School-Manager registrieren.

In diesem Portal sind die Zugänge für das Device Enrollment Program und das Volume Purchase Program für Bildungseinrichtungen zusammengeführt. Innerhalb von VPP erhalten Schulen bei den meisten Apps einen Rabatt, wenn sie mehr als 20 Lizenzen einer App beziehen.

Anmerkung: Die Portale DEP und VPP sind ab Dezember 2019 separat nicht mehr zugänglich. Beides ist bereits im ASM implementiert. Schulen müssen unter Umständen ihre Zugänge zusammenführen.



Vertiefende Informationen und Anleitungen für die Konfiguration der Apple-Dienste finden Sie unter <https://www.apple.com/de/education/>. Der School-Manager wird ausführlich unter <https://www.apple.com/de/education/it/> beschrieben.

4.1.2 Device Enrollment Program - Geräteverwaltung

Mit dem sogenannten „Device Enrollment Program“ DEP lässt sich die Einrichtung von iOS Geräten vereinfachen. Geräte werden bereits beim Kauf einem DEP-Konto der Einrichtung zugewiesen. Das DEP-Inventar wird vom MDM übernommen. Hierdurch wird die Verwaltung der Geräte vereinfacht.

Über DEP werden Einstellungen beim Einrichten der Geräte (Neugeräte oder Geräte-Reset) vorgegeben. Im MDM werden Parameter für die Neueinrichtung hinterlegt, die beim Start eines Gerätes, das sich im Werkszustand befindet, von zentralen Apple-Servern abgerufen werden und an das Gerät übergeben werden.

Hierdurch können viele Konfigurationsschritte (z.B. Einrichtung von Gerätekenwort, Fingerabdruck zum Entsperren, Verknüpfung mit Apple-Konto, ...) übersprungen werden, sodass die Geräteeinrichtung – abhängig von der Methode des Ausrollens – weitestgehend automatisiert werden kann.

4.1.3 Volume Purchase Program – App-Verwaltung

Apple bietet mit dem „Volume Purchase Programm“ (VPP) ein zentrales Werkzeug, über das Schulen Apps beziehen können. Lizenzen können dort eingekauft und ebenfalls an den MDM-Server übergeben werden. Durch Volumenlizenzen ist die App-Zuweisung nicht

abhängig von personalisierten Benutzerkonten wie z.B. bei einem privaten iPad oder Apps aus dem „Windows-Store“.

Mit Hilfe des MDMs werden App-Lizenzen aus dem VPP verwaltet und die Software wird auf die Geräte ausgespielt. Anwendungen können über Standard-Konfigurationen an Geräte verteilt werden, sodass verschiedene Geräte oder verschiedene Anwender(-gruppen) die gleichen Apps erhalten.



Auch kostenlose Apps müssen über VPP lizenziert werden, damit sie an die Endgeräte verteilt werden können.

„Kaufen“ sie die entsprechende App in Ihrem Schulmanager und weisen Sie die Lizenzen Ihrem MDM-Server zu.

Es ist aber auch möglich Apps individuell an Geräte zu verteilen. Hierdurch können kostenintensive Apps oder Apps mit speziellen Funktionen gezielt zugewiesen werden. Wenn eine App nicht mehr auf einem Endgerät genutzt wird, kann die Lizenz entzogen und einem anderen Gerät zugewiesen werden.

4.2 Abbildung von Schulen im School-Manager

Schulträger können eigene Schulen als voneinander unabhängige Organisationseinheiten im School-Manager anlegen und dort je Schule die Geräte (DEP), App-Lizenzen (VPP) und ein MDM anlegen und verwalten.



Abbildung: Modelle für die Umsetzung des Apple-School-Managers

Die Grafik zeigt verschiedene Modelle, wie Schulen in Apples School-Manager abgebildet werden können. Aus Schulträgersicht gibt es zwei Möglichkeiten, wobei die erste Option in zwei Varianten umgesetzt werden kann:

1.a Schulmanager des Schulträgers – keine Differenzierung nach Schulen

Bei diesem Modell legt der Schulträger eine Organisation im ASM an, über die zentral die Verwaltung der Geräte und Lizenzen geschieht.

Über ein MDM können alle Geräte verwaltet und Lizenzen zugewiesen werden.

Vorteile

- Zentrale Verwaltung von Geräten und Lizenzen
- Schulen müssen sich nicht um die Geräteverwaltung im MDM kümmern

Nachteile

- Geringe Flexibilität
- Aufwand beim Schulträger
- Verwaltung der Geräte muss geplant werden (z.B. über Excel-Tabellen muss dokumentiert werden, welche Schule welche Geräte hat)
- Schulen sind auf Schulträger(support) angewiesen

1.b Schulmanager des Schulträgers – Differenzierung nach Schulen

Bei diesem Modell legt der Schulträger eine Organisation im ASM an, über die zentral die Verwaltung der Geräte und Lizenzen geschieht. Schulen werden als „Standorte“ angelegt, sind aber nicht autonom, sondern weiterhin auf Schulträger angewiesen (z.B. beim Erwerb neuer Lizenzen oder neuer Geräte).

Geräte (DEP) werden an Standorte zugewiesen. Lizenzen werden ebenfalls an Standorte verteilt und können dann von den Schulen verwaltet werden.

Bei diesem Modell kann **jede Schule ein eigenes MDM-System** nutzen. Bei der Nutzung eines zentralen MDM-Systems des Schulträgers können Schulen eigene Verwaltungseinheiten erhalten, **sofern das MDM-System mandantenfähig** ist

Vorteile

- Zentrale Verwaltung von Geräten und Lizenzen
- Schulen können MDM selbst konfigurieren
- Höhere Flexibilität

Nachteile

- Aufwand beim Schulträger
- Schulen können nicht selbständig Apps erwerben
- Schulen brauchen Schulträger, um neue Geräte einzupflegen
- Schulen brauchen qualifiziertes Personal für die Bedienung des MDMs

2. Schulmanager der Schule

Bei diesem Modell registriert sich jede Schule individuell bei Apple und pflegt einen eigenen School-Manager. Die Schulen sind damit autonom in der Verwaltung von Geräten und Lizenzen.

Bei diesem Modell kann jede Schule ein eigenes MDM-System nutzen.

Vorteile

- Höchste Flexibilität
- Schulen sind autonom
- Geringer Aufwand beim Schulträger

Nachteile

- Für jede Schule muss eine eigene Infrastruktur geschaffen werden (erhöhter Aufwand).
- Schulen benötigen qualifiziertes Personal.

4.3 Perspektive Android (Google)



In der Verwaltung von Android-Geräten findet aktuell – wie im Folgenden Beschrieben – ein großer Umbruch statt.

Die aktuelle Implementierung von Geräten (und vor allem von Apps) ist umständlich und unserer Meinung nach in der Schule kaum praktikabel. Daher verzichten wir auf eine Beschreibung der aktuellen Verfahren und werden dies in Zukunft nachholen.

Im Februar 2018 hat *Google* mit dem neu aufgelegten Programm „*android enterprise recommended*“ (<https://www.android.com/enterprise/recommended/>) eine Antwort für den Business-Markt gestartet. Google möchte mit diesem Programm Standards für das Geräte-Enrollment setzen.

Über neu entwickelte Google-Dienste, die von MDM-Anbietern implementiert werden können, soll es in Zukunft einfacher werden, die Android-Flotte von Unternehmen zu managen. Mit den kommenden Android-Versionen sollen weitere Features verfügbar gemacht werden.

Um in das Programm aufgenommen zu werden, müssen Hersteller unter anderem folgende Kriterien erfüllen:

- Garantie für zwei Jahre Updates
- Security-Patches nach spätestens 90 Tagen
- Geräte müssen einem Mindeststandard entsprechen

Ein weiterer Schritt Richtung Standardisierung ist „*android one*“ (<https://www.android.com/one>). Hierbei sollen Hersteller ein Standard-Android („*vanilla-like*“) auf den Endgeräten bereitstellen. Es gibt dabei keine Anpassungen an der Benutzeroberfläche und auf zusätzliche Programme („Bloatware“) soll verzichtet werden. Über „*android one*“ wird die Bereitstellung von Security-Patches erleichtert, da

Anpassungen der Hersteller weitgehend wegfallen und *Googles* Updates an die Endgeräte durchgereicht werden können.

Google verspricht eine einfache Einrichtung der Geräte, die in vier Schritten erfolgen soll:

- Geräteerwerb (bei zertifizierten Händlern)
- Zuweisung der Geräte über eine Internetplattform
- Konfiguration über ein MDM-System
- Bereitstellen der Konfiguration bei der Inbetriebnahme der Geräte

Weitere (technische) Informationen finden Sie im Internet unter <https://support.google.com/work/android/answer/7514005>.

Auf der Homepage von „*android enterprise recommended*“ werden unterstützte Geräte aufgelistet (vgl. https://www.android.com/intl/de_de/enterprise/device-collection/#android_enterprise_recommended).

Aktuell befinden sich auf der Homepage nur wenige MDM-Anbieter, darunter *MicroFocus (Novell)*, *Meraki*, *Mobile Iron*.

Die Initiative von *Google* kommt spät, weist aber in die richtige Richtung. Schulen spielen als Zielgruppe aktuell keine Rolle, dies wird sich aber auf absehbare Zeit ändern, wenn Dienstleister Angebote für Schulen erstellen.

5. Fazit

Es besteht eine Diskrepanz zwischen der privaten Nutzung mobiler Endgeräte und dem (professionellen) Einsatz an der Schule. Rechtliche und technische Fragestellungen stellen hohe Anforderungen an die mit der Umsetzung betrauten Kollegen an der Schule.

Heilsbringer, Teufelszeug oder sinnvolle Ergänzung zu bestehenden Unterrichtsmedien? Ob sich der Einsatz mobiler Endgeräte an Ihrer Schule lohnt, müssen Sie letztlich zusammen mit Ihrem Kollegium herausfinden. Bewährte Mechanismen der Medienentwicklungsplanung, Beratungen durch das regionale Medienzentrum und der Austausch mit anderen Schulen helfen Ihnen bei der Entscheidungsfindung.

Agieren Sie bei der Umsetzung Ihrer Tablet-Vorhaben besonnen! Der Anruf einer Schule aus Norddeutschland zeigt exemplarisch, wie schnell Marketingstrategen und Vertriebsmitarbeiter Produkte verkaufen können, deren Nachhaltigkeit fragwürdig ist. An der betroffenen Schule wurden für mehrere zehntausend Euro auf Android basierende Riesen-Tablets an die Wände geschraubt, die Tafeln überflüssig machen sollten. Leider hatte der Hersteller (zum Zeitpunkt des Anrufes) keine Strategie, wie die Geräte zentral mit Software und Updates versorgt werden können.

Dies soll aber nicht entmutigen. Im Gegenteil! Ein guter Unterricht wird durch neue Medien unter Umständen noch besser und der Einsatz von Tablets kann Schüler sicherlich dazu ermutigen selbstständig zu lernen.



Wir freuen uns immer über eine Rückmeldung zu unseren Produkten.

Wenn Sie konkrete Verbesserungsvorschläge zu dieser Anleitung oder zu technischen Rahmenbedingungen haben, nehmen Sie bitte Kontakt mit unserer Hotline auf.

Anhang A: Checkliste



Im Folgenden finden Sie eine Checkliste, die einen Überblick über Aufgaben und Zuständigkeiten geben soll und Ihnen hoffentlich in der Umsetzung behilflich ist.

Einige der hier beschriebenen Arbeitsschritte sind nicht hintereinander, sondern parallel zueinander abzuarbeiten.

Einige dieser Schritte sind optional.

Leider können wir hier keinen Anspruch auf Vollständigkeit erheben – sollten Ihnen fehlende Punkte auffallen, bitten wir um eine Rückmeldung.

1. Verantwortliche

- Wer sind Ihre Ansprechpartner? Wer ist verantwortlich?
- Wurden alle relevanten Gremien informiert und die die Planung einbezogen?

Dienstleister

Schulträger

Kreismedienzentrum

Tablet-Verantwortliche der Schule

Einbeziehung Gesamtlehrerkonferenz?

- Einbeziehung Fachbereiche?
- Einbeziehung Elternbeirat?
- Einbeziehung Schulkonferenz?

2. Finanzierung

- Finanzierung über Schulträger
- Finanzierung über Schuletat
- Sponsoring durch Firmen
- Förderverein
- Leasing
- Finanzierung über Eltern
- Unterstützung für Kinder aus einkommensschwachen Familien

3. Technische Infrastruktur

3.1 Netzwerkkonzept

- In welches Netz werden Geräte eingebunden?
- Internetanbindung
- Strukturierte Verkabelung
- WLAN
- Konfiguration der Firewall
- Jugendschutzfilter

3.2 Gerätehandling

- Gerätelagerung
- Ladestation
- Konfiguration (z.B. über spezielle Tablet-Koffer, ...)
- Lademöglichkeiten im Unterricht
- optional: Caching-Server
- optional: Anbindung der Geräte an die paedML

3.3 Peripherie

- Schutzhüllen
- Stifte
- Tastaturen
- Stative
- Kopfhörer
- Soll von den Geräten präsentiert werden?
- Soll gedruckt werden?

4. Geräteverwaltung

- Auswahl der Geräte
- Registrierung³ beim Hersteller (Apple/Google/Samsung/...)
- Geräte-Beschaffung (achten Sie auf eine Zuweisung der Geräte an die Schule)
- Auswahl MDM-System
- Einrichtung MDM-System

Daten Funktionskonto bei Dienstleister _____

Registrierte Mailadresse: _____

Login-Name: _____

Kennwort: _____

Verantwortliche: _____

Daten Funktionskonto bei Dienstleister _____

Registrierte Mailadresse: _____

Login-Name: _____

Kennwort: _____

Verantwortliche: _____

Daten Funktionskonto bei Dienstleister _____

Registrierte Mailadresse: _____

Login-Name: _____

Kennwort: _____

Verantwortliche: _____

5. Konzepte für den Unterrichtseinsatz

- Wie werden die Geräte im Unterricht eingesetzt?
- Mit welcher Software soll gearbeitet werden?
- Konzept für Datenablage

³ Legen Sie sich ein Funktionskonto an (z.B. tablets@meineschule.de), damit die Verwaltung nicht an eine Person gebunden ist

- Konzept für Protokollierung von Benutzerzugriff
- Gerätesteuerung im Unterricht (z.B. Classroom-App)

6. Fortbildung des Kollegiums

- Lehrer als Multiplikatoren
- Landeslehrerfortbildung
- Kreismedienzentrum
- Dienstleister
- Arbeitskreise
- Schulen aus der Region
- Selbststudium
- Schulinterne Dokumentation (z.B. in eigenem Wiki)
- Sensibilisierung für rechtliche Fragen (Datenschutz, Urheberrecht, ...)

7. Besonderheiten bei Einsatzszenarien

7.1 1:1-Szenario

- Einrichtung von Benutzern im MDM (empfohlen: Pseudonymisierung und keine Klarnamen)
- Dokumentation Gerätezuordnung (z.B. Exceltabelle)
- Rollen/Rechtekonzepte (Welche Gruppen dürfen was?)
- Private Nutzung
- (private) Cloudnutzung (z.B. Datenablage, Einspielen eigener Apps, ...)
- Mailnutzung
- Geräte-Konfiguration durch Nutzer (WLAN, Bluetooth, ...)?
- Konfiguration (Umsetzung der Rollen)
- Optional: Konzept zur Datenspeicherung (außerhalb der Geräte)
- Nutzungsordnung
- Nutzungsverträge
- Versicherung

7.2 1:N-Szenario

- Einrichtung von technischen Benutzern im MDM (z.B. Tablet1 – Tablet N)
- Konzept für Dokumentation Gerätezuordnung (muss bei jedem Benutzerwechsel geschehen)
- Rollen/Rechtekonzepte (Welche Gruppen dürfen was?)
- Konfiguration (Umsetzung der Rollen)
- Nutzung außerhalb der Schule?
- Datenschutz
- Zurücksetzen der Geräte vor Benutzerwechsel
- Konzept zur Datenspeicherung (außerhalb der Geräte)

- Nutzungsordnung
- Nutzungsverträge
- Versicherung

7.3 BYOD

- Verwaltung durch Schule? >>> wenn ja, s. 1:1-Konzept
- Nutzungsordnung
- Versicherung

8. Rechtliche Rahmenbedingungen

- Einverständniserklärungen
- Klärung von Fragen zum Datenschutz
- Verträge mit
 - Lehrern
 - Schülern
 - Eltern
 - Medienzentrum
 - Schulträger
 - Dienstleistern (Auftragsdatenverarbeitung/Wartung/Dienstleistung)
 - MDM-Hersteller
 - Versicherungen
 - App-Anbieter
- Nutzungsordnungen
- Verarbeitungsverzeichnis (vormals: Verfahrensverzeichnis)

Anhang B: Weiterführende Links

- Hinweise zu mobilen Endgeräten an Schulen in BW/Muster-Nutzungsordnung – <https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/mobile>
- Hinweise zu Verfahrensverzeichnissen – https://lehrerfortbildung-bw.de/st_recht/daten/ds_neu/verfahren/
- Hinweise zur Auftragsdatenverarbeitung – https://lehrerfortbildung-bw.de/st_recht/daten/ds_neu/auftrag/
- Übersicht zu Urheberrecht und Datenschutz bei der Lehrerfortbildung BW – https://lehrerfortbildung-bw.de/st_recht/
- Inhalte im Kultusportal zum Datenschutz an Schulen - <https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Datenschutz+an+Schulen>
- Hinweise im Kultusportal zum Einsatz mobiler Endgeräte - <https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/mobile>
- Informationen zum Datenschutz für Schulen in NRW (Achtung! Beachten Sie, dass unter Umständen in Baden-Württemberg abweichende Vorschriften gelten!) – <https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/index.html>
- PDF „Apple im Bildungsbereich Überblick Datenschutz und Privatsphäre für Schulen“ – https://www.apple.com/de/education/docs/Data_and_Privacy_Overview_for_Schools.pdf
- iOS-Implementierung: Referenz – <https://help.apple.com/deployment/ios/#/>
- Implementierungsreferenz iOS für den Bildungsbereich – <https://help.apple.com/deployment/education/?lang=de#/>
- Hilfe zu Apple School-Manager: <https://help.apple.com/schoolmanager/?lang=de#/>
- Einstellungen für die Mobilgeräteverwaltung für IT – <https://help.apple.com/deployment/mdm/>
 - Insbesondere „MDM-Befehle“ – <https://help.apple.com/deployment/mdm/#/mdm789N2K1QP>
- Classroom-App– https://images.apple.com/chde/education/docs/getting-started-with-classroom-2.0_de-CH.pdf
- Einführende Artikelserie im Support-Netz – <https://www.lmz-bw.de/netzwerkloesung/fachwissen/tablets-in-der-schule/>
- Handreichung „Im digitalen Zeitalter qualitätsorientiert lernen. Chancen und Grenzen digitaler Medien.“ – <http://www.schule-bw.de/themen-und-impulse/uebergreifende-erziehung/medienerziehung/handreichungen/basisband>

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111
70190 Stuttgart

© Landesmedienzentrum Baden-Württemberg, 2019