Empfehlung für die Konfiguration von unpersonalisierten in der Schule genutzten iPads

Es geht um iPads, die von wechselnden Schülerinnen und Schülern (SuS) genutzt werden. Teilweise können die Geräte für eine längere Zeit bei einer Lerngruppe verbleiben. Eine Anmeldung an den Geräten ist nicht vorgesehen und sollte auch aktiv unterbunden werden, da dadurch Risiken entstehen können, wenn SuS vergessen, sich abzumelden.

Einschränkungen, die Funktionen betreffen, welche nur mit einer Anmeldung am Gerät verfügbar sind, sollten trotzdem genutzt werden, um diese Funktionen sicherheitshalber einzuschränken. Das betrifft u.a. auch die iCloud, deren Nutzung immer an eine (managed) Apple ID gekoppelt ist.

Einige Funktionen wie Home, Wallet oder Stocks, die für Schülerinnen und Schüler ohnehin nicht nutzbar sind, sollten über eine Blacklist von den Geräten entfernt werden, um Ablenkungen zu vermeiden (Positiv- und Negativliste im MDM).

Nutzen Schülerinnen und Schüler iPads eventuell auch über eine längere Zeit und speichern Ergebnisse auf den Geräten selbst, muss vor der Abgabe der Geräte für eine Nutzung durch andere SuS, z.B. einer anderen Klasse, sichergestellt sein, dass diese Inhalte von den Geräten gelöscht und an anderer Stelle gespeichert werden (NextCloud, Schulserver, NAS, USB Stick, Lehrergerät, etc.).

Thema **Sicherheit**. Die Wahrscheinlichkeit, dass über ein iOS Gerät ein lokales Netzwerk kompromittiert wird oder andere Geräte im gleichen Netzwerk, ist - verglichen mit Windows Geräten - extrem gering. Trotzdem sollte sichergestellt werden, dass Updates zeitnah auf alle Geräte kommen. App-Updates müssen in der MDM Verwaltung manuell angestoßen werden. Dies sollte wöchentlich außerhalb der Schulzeit geschehen. Falls der Schulträger keine Firewall im Einsatz hat, sollte in den Profileinstellungen des MDM der “Filter für Webinhalte” aktiviert werden. Hier gibt es verschiedene Konfigurationsmöglichkeiten.

Da die Geräte nicht personalisiert sind, sind die Sicherheitsanforderungen zum Schutz von (personenbezogenen) Daten auf dem Gerät deutlich geringer als bei personalisierten Geräten. Die größten Risiken entstehen durch die Nutzer selbst, etwa wenn sie Daten auf dem Gerät speichern oder an andere Nutzer übermitteln.

Die folgenden Empfehlungen versuchen die Interessen aller Beteiligten - Lehrkräfte, Schulträger, Schulleitungen, Datenschutzbeauftragte - zu berücksichtigen.

Hinweis: Aus Platzgründen wird “Schülerinnen und Schüler” teilweise mit SuS abgekürzt.

Version 1.02
Stand 24.05.2023

iOS/ iPad OS 16.2

Die beschriebenen Einschränkungen (Payloads) orientieren sich an den in JamfSchool verfügbaren. Dieses setzt die in iOS und iPad OS 16.2 verfügbaren Einschränkungen sehr umfänglich um. Andere MDM stellen eventuell nicht alle diese Einschränkungen bereit, wie etwa das von IServ. In Relution sollten die Einschränkungen in ähnlichem Umfang verfügbar sein.

Übersicht zu verschiedenen iOS Funktionen und Datenschutz https://www.apple.com/de/legal/privacy/data/

In Spalte 2 geben die Tabellen an, ob ein Haken gesetzt sein muss oder nicht, um die jeweilige Einschränkung im Sinne dieser Empfehlung zu aktivieren oder deaktivieren.

Gerätefunktionen

Damit erlaubte Punkte aus dieser Liste funktionieren, müssen ggf. **TCP- und UDP-Ports** freigegeben werden. Diese sind hier aufgeführt: https://support.apple.com/de-de/HT202944

Payload		**Auswirkung der Einschränkung wo wichtig**	**Erforderlich für den Unterricht?**	**Relevanz für die Sicherheit** **a) von personenbezogenen Daten** **b) der Schul IT Infrastruktur**
Verwenden der Kamera erlauben	☑		**Ja**, z.B. zum Erstellen von Medienprodukten. Bezug zu MKR 4.1 Zum Erfassen von QR-Codes erforderlich.	a) Relevant, da Bilder personenbezogene Daten enthalten können. Bezug zu MKR 1.4 Problem von auf dem Gerät verbleibenden Bildern. Unbedenklich, solange Bilder sicher gespeichert werden, z.B.

				Nextcloud, oder bei Weitergabe der Geräte an eine andere Klasse gelöscht werden.
Sprachwahl erlauben	▢	Benutzer können bei gesperrtem Gerät keine Sprachbefehle verwenden, um Telefonnummern zu wählen, wenn nicht erlaubt.	**Nein**, keine Relevanz bei iPads.	Keine Relevanz
FaceTime erlauben	▢		**Nein,** Schulen verwenden hier alternative Plattformen.	a) Wird aus Datenschutzgründen nicht verwendet.
Bildschirmaufnahmen erlauben	☑		**Ja**, wird z. B. für die Erstellung von Erklärvideos benötigt. Bezug zu MKR 4.1	a) Relevant, da Bildschirmaufnahmen personenbezogene Daten enthalten können. Bezug zu MKR 1.4 Problem von auf dem Gerät verbleibenden Screenshots mit personenbezogenen Inhalten. Unbedenklich, solange die Aufnahmen sicher gespeichert werden, z.B. Nextcloud, oder bei Weitergabe der Geräte an eine andere Klasse gelöscht werden.
Bildschirmbeobachtung über Classroom erlauben	☑		**Ja**, zur Unterstützung der SuS bei der Bedienung der Geräte und - falls notwendig - auch zur Überwachung. Erforderlich, wenn Bildschirminhalt auf Apple TV gespiegelt werden soll, ohne Freigabe für SuS selbst.	a) Relevant, da Überwachung personenbezogene Daten enthalten kann. SuS vorab über Möglichkeit und Anwendung informieren Bezug zu MKR 1.4

Automatisches Synchronisieren beim Roaming erlauben	☐		**Nein**, nicht relevant	Keine Relevanz
Installation von Apps erlauben	☐	Die Installation setzt voraus, dass SuS sich am Gerät mit einer (privaten)Apple ID anmelden können.	**Nein**, Schülerinnen und Schüler dürfen keine Apps installieren.	a) Relevant, da nicht autorisierte Apps personenbezogene Daten verarbeiten können
Entfernen von Apps erlauben	☐		**Nein**, Schülerinnen und Schüler dürfen keine Apps entfernen.	a) Relevant, da Apps personenbezogene Daten enthalten können
In-App-Käufe erlauben	☐	Setzt die Anmeldung mit einer privaten Apple ID voraus.	**Nein,** nicht relevant	Keine Relevanz.
Siri erlauben	☑ ☐	Siri greift zum Umsetzen von Befehlen und Fragen zunächst auf die Ressourcen auf dem Gerät zurück. Reicht dieses nicht aus, greift Siri auf Apple Dienste in der Cloud zu. Das erfolgt mit einer anonymisierten ID, die regelmäßig wechselt. Siri kann eine Hilfe für Nutzer mit Einschränkungen sein und sollte dort in Kopplung mit einer privaten Apple ID genutzt werden.	**Bedingt**, erweitert die Funktionalität des Gerätes, kann aber auch zu Unterrichtsstörungen führen. Bezug zu MKR 2.1	a) Relevant, da Siri personenbezogene Daten verarbeiten kann. Sollte auf unpersonalisierten Geräten aber nicht ins Gewicht fallen.
Installieren von Rapid Security Response erlauben	☑	Gibt Apple die Möglichkeit, Bug Fixes auszurollen, ohne dass ein vollständiges Update installiert werden muss.	**Ja**, zur Verbesserung der Sicherheit	a) Keine Relevanz. b) Relevant, da die Sicherheit des Systems erhöht wird.
Einschränkungen/ Bildschirmzeit erlauben	☐		**Nein**, kann zu Störungen in der Gerätefunktion im Unterricht führen. Bezug zu MKR 5.4	Keine Relevanz
Fortsetzen von Aktivitäten (Handoff) erlauben	☐		**Nein**, bei unpersonalisierten Geräten nicht erforderlich.	Keine Relevanz

Nachschlagen im Wörterbuch erlauben	☑	Die Wörterbücher an sich laufen komplett offline.	**Ja**, für Recherche im Unterricht Bezug zu MKR 2.1	a) Bedingt relevant, da Recherche personenbezogene Daten verarbeiten kann
QuickType Textvorschläge erlauben	☑	Zeichnet anonymisiert Daten auf, nicht mit einer managed Apple ID verknüpft.	**Ja**, als Unterstützung für SuS beim Schreiben	a) Bedingt relevant, da Texte personenbezogene Daten enthalten können
Auto-Korrektur erlauben	☑		**Ja**, als Unterstützung für SuS beim Schreiben	a) Bedingt relevant, da Texte personenbezogene Daten enthalten können
Rechtschreibprüfung erlauben	☑		**Ja**, als Unterstützung für SuS beim Schreiben	a) Bedingt relevant, da Texte personenbezogene Daten enthalten können
AirDrop erlauben	☑	AirDrop ermöglicht unkompliziert das kooperative Arbeiten zwischen den SuS. Ein Kind, das Fotos gemacht hat, kann diese mit anderen Geräten in der Klasse teilen, damit sie dort von den SuS weiter bearbeitet werden und so etwa verschiedene Fotocollagen entstehen. Wird AirDrop nicht erlaubt, sollte eine Alternative zum Teilen angeboten werden, beispielsweise ein Messenger oder eine Cloud-Lösung mit App-Einbindung (in beiden Fällen datenschutzkonform und sicher).	**Ja**, wird im Unterricht zum Verteilen und Einsammeln von Materialien genutzt Bezug zu MKR 3.1	a) Relevant, da AirDrop personenbezogene Daten auch an fremde Geräte teilen kann Bezug zu MKR 1.4 b) Es besteht ein geringes Risiko, Schadsoftware über AirDrop zu empfangen, da AirDrop immer nur für 10 Minuten “für alle” geöffnet werden kann. Schadsoftware ist auf iOS Geräten ein geringes Problem. Risiken entstehen, wenn Schadsoftware von iPads auf Windows Geräte gelangt. Bei Koffergeräten ist das Szenario unwahrscheinlich.

AirDrop als nicht verwaltetes Ziel behandeln	☐	Benutzern wird AirDrop in einer verwalteten App als Option angeboten. Ist diese Einschränkung aktiviert, muss die Option „Dokumente von verwalteten Quellen in nicht verwalteten Zielen erlauben“ deaktiviert werden (also ohne Haken), damit sie funktioniert. Haken erzwingt, dass AirDrop als nicht verwaltetes Drop-Ziel betrachtet wird. Es hindert verwaltete Anwendungen daran, Daten über Airdrop zu senden. Bei gesetztem Haken wird das Teilen mit anderen Geräten in der Klasse deutlich eingeschränkt. Es ist dann nicht mehr möglich, Inhalte in verwalteten Apps mit anderen Geräten zu teilen.	**Nein**, da viele im Unterricht genutzte Apps verwaltet sind und Inhalte so nicht mit der Lehrkraft (falls erforderlich) oder mit anderen SuS geteilt werden können.	a) Relevant, da AirDrop personenbezogene Daten auch mit fremden Geräten teilen kann Bezug zu MKR 1.4 b) Das Empfangen von Daten über AirDrop ist bei gesetztem Haken nur noch eingeschränkt möglich. Ist AirDrop zugelassen, ist es bei Koffergeräten unerheblich, mit welchen Apps Teilen darüber zulässig ist.
Spotlight Vorschläge erlauben	☑ ☐		**Bedingt**, als Unterstützung bei der Suche nach Informationen.	a) Bedingt relevant, da Suchanfragen personenbezogene Daten enthalten können, diese hier aber mit keiner Person verbunden sind
Diktierfunktion erlauben	☑	**Diktieren mit Siri verhindern** muss aktiviert sein, damit die Funktion komplett offline läuft.	**Ja,** möglich. Kein Datenschutz Problem, wenn offline. Bezug zu MKR 4.2	a) Relevant, da Texte personenbezogene Daten enthalten können
Diktieren mit Siri verhindern	☑ ☐	Wenn nicht verhindert, werden verschlüsselte Protokolle an Apple Server gesendet, die dann mit einer zufälligen, auf dem Gerät generierten Kennung verknüpft sind.	**Bedingt**, Diktieren ist auch ohne Siri möglich (s.o.).	a) Relevant, da Siri personenbezogene Daten verarbeiten kann

		Achtung! Standardmäßig können Benutzer bei vielen Apps und Funktionen, die die Tastatur auf Geräten verwenden, Text per Diktat eingeben. Das geht u.U. **nicht**, wenn die Einschränkung aktiviert wird.	Bei SuS mit Beeinträchtigungen kann die Funktion zur Nutzung von Apps mit Texteingabe wichtig sein.	
Verhindern von Verbindungen zu Siri Servern für Übersetzungen	☑	Die Übersetzung erfolgt dann ausschließlich auf dem Gerät selbst.	**Ja**, um unbeabsichtigte Übertragung von Sprachaufnahmen zu verhindern.	a) Relevant, da Siri personenbezogene Daten verarbeiten kann
Koppeln mit anderen Computern erlauben	▢		**Nein**, im Unterricht nicht erforderlich.	a) Relevant, da Datenübertragungen personenbezogene Daten enthalten können b) Relevant, da Schadsoftware eingeschleust werden kann
Modus für eingeschränkten Zugriff über USB erlauben	▢	Erlaubt die Kopplung mit USB Geräten auch wenn der Bildschirm gesperrt ist. Die Verbindung bleibt aufrechterhalten, wenn der Bildschirm gesperrt wird. Dieses kann sinnvoll sein, wenn Zubehör am iPad aufgeladen werden soll, etwa ein Stift oder eine Tastatur, die über USB/ Lightning angeschlossen wird. Damit der USB Port auch bei Bildschirmsperre offen bleibt, darf der Haken **nicht** gesetzt sein!!! “Erlauben” ist hier im Sinne von Vorschreiben zu verstehen.		Geringe Relevanz bei Hardware, welche kein Speichermedium ist.
Zugriff auf USB-Laufwerke in Dateien App erlauben	☑ ▢	Kann in einigen Settings erforderlich sein, um Daten auf einen USB Stick zu speichern.	**Ja**, als Unterstützung für Datenaustausch, falls USB Sticks dafür genutzt werden.	a) Relevant, da Datenübertragung

				personenbezogene Daten enthalten kann b) Relevant, da Schadsoftware eingeschleust werden kann
Nahfeldkommunikation (NFC) zulassen	▢		**Nein**, kann unbefugten Zugriff ermöglichen.	a) Relevant, da NFC personenbezogene Daten enthalten kann

Sperrbildschirm				
Payload		**Auswirkung der Einschränkung wo wichtig**	**Erforderlich für den Unterricht?**	**Relevanz für die Sicherheit** **a) von personenbezogenen Daten** **b) der Schul IT Infrastruktur**
Kontrollzentrum auf Sperrbildschirm anzeigen	▢	Setzt Anmeldung mit Apple ID voraus.	**Nein**	a) Bedingt relevant, da Zugriff personenbezogene Daten preisgeben kann
Mitteilungszentrale auf Sperrbildschirm anzeigen	▢	Setzt Anmeldung mit Apple ID voraus.	**Nein**	a) Bedingt relevant, da Benachrichtigungen personenbezogene Daten enthalten können
Ansicht "Heute" auf Sperrbildschirm anzeigen	▢	Setzt Anmeldung mit Apple ID voraus.	**Nein**	a) Bedingt relevant, da Ansicht personenbezogene Daten enthalten kann

Passbook Mitteilungen auf Sperrbildschirm anzeigen	▢	Setzt Anmeldung mit Apple ID voraus.	**Nein**	a) Bedingt relevant, da Zugriff personenbezogene Daten preisgeben kann

Anwendungen				
Payload		**Auswirkung der Einschränkung wo wichtig**	**Erforderlich für den Unterricht?**	**Relevanz für die Sicherheit a) von personenbezogenen Daten b) der Schul IT Infrastruktur**
Verwenden des iTunes Store erlauben	▢	Setzt Anmeldung mit Apple ID voraus.	**Nein**	a) Relevant, da bei Nutzung des iTunes Stores personenbezogene Daten verarbeitet werden.
Verwenden von Safari erlauben	☑	Ohne Haken: Der Webbrowser Safari wird deaktiviert und sein Symbol wird aus dem Home-Bildschirm entfernt. Diese Einstellung hindert Benutzer auch daran, Webclips zu öffnen.	**Ja**, für Recherche im Unterricht Bezug zu MKR 2.1	a) Relevant, da über den Browser personenbezogene Daten verarbeitet werden können. Hier muss insb. mit den Schülerinnen und Schülern besprochen werden, dass persönliche Daten im Internet nur mit Rücksprache der Lehrperson preisgegeben werden dürfen. Bezug zu MKR 1.4

				b) Für eine möglichst sichere Nutzung von Safari sind die Unterpunkte zu beachten.
Automatisches Einfügen aktivieren	▢	Benutzereingaben in Webformularen werden von Safari nicht für die nochmalige Verwendung aufbewahrt.	**Nein**, da so nachfolgende SuS Inhalte, welche SuS vor ihnen eingegeben haben, sehen könnten	a) Relevant, da personenbezogene Daten von Vornutzern enthalten sein können
JavaScript aktivieren	☑	Ohne Haken: Safari ignoriert alle Vorkommen von JavaScript auf Websites.	**Ja**, für Funktionen auf Webseiten	b) JavaScript läuft in vielen Websites, kann u.U. ein Sicherheitsrisiko sein. In iOS Risiko aber eher gering.
Deaktivieren des Pop-Up-Blockers durch Benutzer erlauben	☑		**Ja**, Pop-ups sind heute eher selten. Einige Websites nutzen es für Authentifizierung. In solchen Fällen sollte man es gegebenenfalls aktivieren können.	Geringe Relevanz
Betrugswarnung erzwingen	☑		**Ja**, zur Verbesserung der Sicherheit	a) Relevant, da mehr Sicherheit personenbezogene Daten schützen kann
Cookies akzeptieren ↓	4 Opti-onen	Die folgenden vier Optionen können gewählt werden.	**Nein**, für Funktionen auf Webseiten	a) Relevant, da Cookies personenbezogene Daten enthalten können
Die Optionen "Websiteübergreifende s Tracking verhindern" und "Alle Cookies blockieren" sind aktiviert und können	Aus wahl	Das Blockieren von Cookies kann die Funktion einzelner Websites beeinträchtigen.	**Ja**, zum Schutz der Privatsphäre	a) Relevant, da Tracking und Cookies personenbezogene Daten enthalten können

vom Benutzer nicht deaktiviert werden.				
Die Option "Websiteübergreifendes Tracking verhindern" ist aktiviert und kann vom Benutzer nicht deaktiviert werden.			**Nein**	s.o.
"Die Option Alle Cookies blockieren" ist deaktiviert, kann vom Benutzer jedoch deaktiviert werden.			**Nein**	s.o.
Die Option "Websiteübergreifendes Tracking verhindern" ist aktiviert, die Option "Alle Cookies blockieren" ist jedoch deaktiviert. Beide Einstellungen können vom Benutzer geändert werden.			**Nein**	s.o.
Automatische App-Downloads erlauben	☑		**Ja**, relevant, sofern die Installation von Apps erlaubt ist.	Geringe Relevanz
iMessage erlauben	▢		**Nein**, es werden alternative Messenger verwendet.	a) Relevant, da Nachrichten personenbezogene Daten enthalten können

Synchronisieren von Notizen und Hervorhebungen in unternehmenseigenen Büchern erlauben	☐		**Nein**, da Geräte nicht personalisiert	a) Relevant, da Notizen personenbezogene Daten enthalten können
Podcasts erlauben	☑ ☐		**Bedingt**, da andere Quellen für Podcasts über den Browser abrufbar sind. Bezug zu MKR 5.4 Podcasts ist auch ohne Anmeldung mit (managed) Apple ID nutzbar.	a) ohne Anmeldung mit (managed) Apple ID nicht relevant
"Mein Gerät suchen" in der Suche-App erlauben	☐		**Nein**	a) Relevant, da Ortung personenbezogene Daten enthalten kann
"Meine Freunde suchen" in der Suche-App erlauben	☐		**Nein**	a) Relevant, da Ortung personenbezogene Daten enthalten kann
Game Center erlauben	☐		**Nein**, kann Ablenkung im Unterricht verursachen.	Geringe Relevanz
Book Store erlauben	☐		**Nein**, Inhalte werden von Schule bereitgestellt. Kann zu Ablenkung führen.	a) Relevant, da Book Store personenbezogene Daten verarbeiten kann
Apple Music erlauben	☐		**Nein**, kann Ablenkung im Unterricht verursachen.	Geringe Relevanz
Apple News erlauben	☐		**Nein**, nicht erforderlich	a) Relevant, da Apple News personenbezogene Daten verarbeiten kann

Entfernen von System-Apps erlauben	▢		**Nein**, kann die Funktion des Geräts beeinträchtigen.	Geringe Relevanz
Einstufen neuer Entwickler unternehmenseigener Apps als vertrauenswürdig erlauben	▢		**Nein**, wäre nur relevant, wenn eine Schule eigene Apps entwickelt.	Geringe Relevanz
Schreiben von Kontaktdaten in Kontakte nicht verwalteter Accounts durch verwaltete Apps erlauben iOS ab Version 12	▢		**Nein**, für Unterricht nicht erforderlich. Auf Koffergeräten nicht relevant, da es eine Anmeldung mit managed Apple ID voraussetzt.	a) Relevant, da Kontaktdaten personenbezogene Daten enthalten können
Lesen von Kontaktdaten in Kontakten nicht verwalteter Accounts durch verwaltete Apps erlauben iOS ab Version 12	▢		**Nein**, für Unterricht nicht erforderlich. Auf Koffergeräten nicht relevant, da es eine Anmeldung mit managed Apple ID voraussetzt.	a) Relevant, da Kontaktdaten personenbezogene Daten enthalten können
Software-Updates zurückstellen für **10** Tage	☑		**Ja**, um Unterrichtsstörungen durch fehlerhafte Updates zu vermeiden. Ausnahme: Sicherheits-Updates.	b) Relevant, um sicherzustellen, dass Updates nicht zu Funktionseinschränkungen führen.

iCloud

Bei Koffergeräten ohne Personalisierung (z.B. Shared iPad) und ohne Möglichkeit der Anmeldung mit privater Apple ID wird iCloud nicht genutzt/ ist ein Zugriff auf iCloud nicht möglich.

Payload		Auswirkung der Einschränkung wo wichtig	Erforderlich für den Unterricht?	Relevanz für die Sicherheit a) von personenbezogenen Daten b) der Schul IT Infrastruktur
Sichern in iCloud erlauben	☐	Auf Koffergeräten nicht relevant, da es eine Anmeldung mit managed Apple ID voraussetzt.	**Nein**	a) Relevant, da iCloud personenbezogene Daten speichert
iCloud Dokumente und Daten erlauben	☐	s.o.	**Nein**	a) Relevant, da iCloud personenbezogene Daten speichert
iCloud Schlüsselbund erlauben	☐	s.o.	**Nein**	a) Relevant, da iCloud personenbezogene Daten speichert
iCloud Fotomediathek erlauben	☐	s.o.	**Nein**	a) Relevant, da iCloud personenbezogene Daten speichert
Synchronisieren verwalteter Apps mit iCloud erlauben	☐	s.o.	**Nein**	a) Relevant, da iCloud personenbezogene Daten speichert
Fotostream erlauben	☐	s.o.	**Nein**	a) Relevant, da Fotostream personenbezogene Daten speichert
Gemeinsamen Fotostream erlauben	☐	s.o.	**Nein**	a) Relevant, da Fotostream personenbezogene Daten speichert

iCloud Privat Relay erlauben iOS 15 oder neuer	▢	s.o.	**Nein**	a) Relevant, da Privat Relay personenbezogene Daten schützen kann

Sicherheit und Datenschutz

Payload		**Auswirkung der Einschränkung wo wichtig**	**Erforderlich für den Unterricht?**	**Relevanz für die Sicherheit** **a) von personenbezogenen Daten** **b) der Schul IT Infrastruktur**
Touch ID das Entsperren des Geräts erlauben	▢		**Nein**	Geringe Relevanz
Senden von Diagnosedaten an Apple erlauben	▢		**Nein**	Geringe Relevanz
Dokumente aus verwalteten Apps in nicht verwalteten Apps erlauben	☑	Die Einstellung (ohne Haken) ist sinnvoll in einem Bring-Your-Own-Device Einsatzszenario. Hier wird dann verhindert, dass Daten aus einem verwalteten Kontext (Apps, die in der Schule genutzt werden) in einen nicht verwalteten Kontext gelangen (Apps, die privat genutzt werden). Sinnvoll ist dann zusätzlich der Haken bei “AirDrop als nicht verwaltetes Ziel behandeln”. Bei entferntem Haken wird das App-übergreifende Teilen von Dateien deutlich eingeschränkt. Es kann dann beispielsweise nicht mehr ohne Weiteres in der Dateien-App gespeichert werden.	**Ja.** Ermöglicht das Verwalten und Teilen von Dateien mit der Dateien App. Ermöglicht bzw. erleichtert das App-übergreifende Arbeiten. Bezug zu MKR 1.3 und 4.4	a) bei schulischen Geräten, auf denen keine privaten Apps installiert werden können geringe Relevanz Problem von auf dem Gerät verbleibenden Dateien mit personenbezogenen Inhalten. Unbedenklich, solange diese Dateien sicher gespeichert werden, z.B. Nextcloud, oder bei Weitergabe der Geräte an

		In so einem Fall sollte eine Alternative zum Speichern angeboten werden (z. B. eine datenschutzkonforme und sichere Cloud-Lösung mit App-Einbindung).		eine andere Klasse gelöscht werden. b) s. a) geringe Relevanz, da es keine privat installierten Apps auf den Geräten gibt
Dokumente aus nicht verwalteten Apps in verwalteten Apps erlauben	☑	s.o.	**Ja**, s.o.	s.o.
Sicherstellen, dass die Kopier- und Einfügefunktion die Beschränkungen für verwaltete/unverwaltete Dokumente beachtet	☐ ☑	s.o.	**Bedingt**, nur relevant (mit Haken), wenn Dokumente aus verwalteten Apps in nicht verwalteten Apps - und umgekehrt - nicht erlaubt sind (also ohne Haken).	s.o.
Verschlüsselte Sicherungen erzwingen	☐		**Nein**, da unpersonalisierte Geräte keine Sicherung erlauben	Keine Relevanz
Beschränktes Ad-Tracking erzwingen	☑		**Ja**, um Werbung einzuschränken, auch wenn auf unpersonalisierten Geräten eher nicht von Bedeutung.	a) Relevant, da personenbezogene Daten betroffen sein können
Eingabe eines iTunes Store Passworts für alle Einkäufe durch den Benutzer durchsetzen	☑		**Ja**, um unautorisierte Käufe zu verhindern - falls der iTunes-Store erlaubt ist.	a) Relevant, da personenbezogene Daten betroffen sein können
Verwendung eines Passworts beim Erhalt von AirPlay Kopplungsanfragen von diesem Gerät auf anderen Geräten durchsetzen	☑		**Ja**, um unbefugtes AirPlay-Streaming zu verhindern	a) Relevant, da personenbezogene Daten betroffen sein können

Ändern des Codes erlauben	☐	Wenn zugelassen, können Schüler Geräte sperren und Nutzung verhindern.	**Nein**, um Missbrauch zu vermeiden	a) Keine Relevanz
Ändern von Touch ID Fingerabdrücken / Face ID Gesichtern erlauben	☐	Wenn zugelassen, können Schüler Geräte sperren und Nutzung verhindern.	**Nein**, da Geräte nicht personalisiert	a) Relevant, da personenbezogene Daten betroffen sein können
E-Mail-Datenschutz für Geräte zulassen	☑	Ohne Nutzeranmeldung nicht relevant.	**Ja**, um E-Mails zu schützen.	a) Relevant, da E-Mails personenbezogene Daten enthalten können
Automatisches Einfügen von Passwörtern erlauben	☐	Greift auf die in Keychain gespeicherten Passwörter zurück, sofern ein Nutzer am Gerät angemeldet ist.	**Nein**, ohne managed Apple ID ohne Wirkung	Geringe Relevanz
Vor automatischem Einfügen Authentifizierung erforderlich	☑		**Ja**, um unautorisiertes Einfügen von Passwörtern zu verhindern. Für Koffergeräte letztlich nicht relevant.	a) Relevant, da Passwörter personenbezogene Daten schützen
Abfrage von Passwörtern auf Geräten in der Nähe erlauben	☐		**Nein**, für Schulgeräte nicht erforderlich.	a) Relevant, da Passwörter personenbezogene Daten schützen
Passwortfreigabe über AirDrop erlauben	☐		**Nein**	a) Relevant, da Passwörter personenbezogene Daten schätzen
Nicht vertrauenswürdige TLS-Verbindungen mit Bestätigung erlauben	☑ ☐		**Bedingt**, sofern eine Firewall ausreichende Absicherung bietet. Fall nicht, keinen Haken setzen.	Geringe Relevanz

Interessenbezogene Werbung von Apple erlauben	▢		**Nein**, für den Unterricht nicht erforderlich.	Geringe Relevanz
Sichern unternehmenseigener Bücher erlauben	☑		**Ja**, um Daten zu schützen	a) Relevant, da Bücher personenbezogene Daten enthalten können
Automatische Updates von Einstellungen für vertrauenswürdige Zertifikate erlauben	☑		**Ja**, um die Sicherheit zu verbessern.	a) Relevant, da personenbezogene Daten betroffen sein können
Starten von Geräten im Wiederherstellungsmodus mit einem nicht gekoppelten Gerät, das über ein Lightning Kabel angeschlossen ist, erlauben	☑ ▢	Wenn diese Einstellung aktiviert ist, können Benutzer iOS- oder iPad OS-Geräte von einem externen Host-Computer (ungekoppelter Host) in den Wiederherstellungsmodus starten. Standardmäßig kann ein externer Host-Computer ein Gerät nicht im Wiederherstellungsmodus starten. An vielen Schulen werden mit den iPads keine Computer gekoppelt sein. Es kann u.U. die einzige Möglichkeit sein, ein iPad wieder in Gang zu setzen, wenn es über MDM nicht mehr ansprechbar ist.	**Ja**, um den Wiederherstellungsprozess zu erleichtern. Muss von Schule zu Schule entschieden werden.	a) Relevant, da personenbezogene Daten betroffen sein können b) Über diese Möglichkeit könnte ein iPad seine Daten verlieren.
Autonomer Einzel-App-Modus		Wird in dem Textfeld eine App definiert, kann nur noch diese geöffnet werden. Bleibt das Feld leer, sind alle Apps verfügbar.	**Ja**, um den Gerätezugriff bei Bedarf zu beschränken	a) Relevant, da personenbezogene Daten betroffen sein können

AirPrint				
Payload		**Auswirkung der Einschränkung wo wichtig**	**Erforderlich für den Unterricht?**	**Relevanz für die Sicherheit** **a) von personenbezogenen Daten** **b) der Schul IT Infrastruktur**
AirPrint erlauben	☑		**Ja**, um Drucken zu ermöglichen. Bezug zu MKR 4.1	a) Relevant, da gedruckte Daten personenbezogene Daten enthalten können
Speichern der Anmeldedaten für AirPrint im Schlüsselbund erlauben	☐		**Nein**, auf unpersonalisierten Geräten gibt es keinen Schlüsselbund.	a) Relevant, da Zugangsdaten personenbezogene Daten enthalten können
Vertrauenswürdiges Zertifikat für TLS-Verbindung mit Druckern erzwingen Nur betreute Geräte, iOS ab Version 11	☑		**Ja**, um sichere Verbindungen zu gewährleisten.	a) Relevant, da personenbezogene Daten übertragen werden können
Suche nach AirPrint Druckern per iBeacon erlauben Nur betreute Geräte, iOS ab Version 11	☑		**Ja**, um Drucken zu erleichtern.	Geringe Relevanz

Klassenzimmer (Classroom)				
Payload		**Auswirkung der Einschränkung wo wichtig**	**Erforderlich für den Unterricht?**	**Relevanz für die Sicherheit** **a) von personenbezogenen Daten** **b) der Schul IT Infrastruktur**
Classroom erlauben, für vom Administrator erstellte Klassen für iOS 10 oder älter „Bildschirm anzeigen“ ohne Nachfrage auszuführen	☑	Wenn der Haken gesetzt ist, können Lehrkräfte mit ihrem Dienst-iPad die Schülergeräte ihrer Lerngruppe über die Classroom-App als Gruppe einrichten und haben dadurch Zugriff auf die Geräte der SuS..	**Ja**, um Schülerinnen und Schüler bei der Arbeit am Gerät zu unterstützen und bei Bedarf zu überwachen.	a) Relevant, da personenbezogene Daten übertragen werden können
Beschränken auf App und Sperren des Geräts in Classroom ohne Bestätigung erlauben	☑	Wenn Haken gesetzt, benötigt es keiner Zustimmung des Zugriffs durch die SuS.	**Ja**, um Schülerinnen und Schüler bei der Arbeit am Gerät zu unterstützen und bei Bedarf zu überwachen.	a) Relevant, da personenbezogene Daten übertragen werden können
Classroom Klassen ohne Bestätigung automatisch beitreten	☑	s.o.	**Ja**, um Schülerinnen und Schüler bei der Arbeit am Gerät zu unterstützen und bei Bedarf zu überwachen.	a) Relevant, da personenbezogene Daten übertragen werden können

Bei einer von einer Lehrkraft in der Classroom App von Apple erstellten Klasse das Verlassen der Klasse ohne die Erlaubnis der Lehrkraft verhindern	☑	Bei nicht gesetztem Haken können sich SuS unbemerkt der Überwachung entziehen.	**Ja**, um zu verhindern, dass Schülerinnen und Schüler die Gruppe ohne Zustimmung durch die Lehrkraft verlassen können.	a) Relevant, da personenbezogene Daten übertragen werden können

Verbindung

Payload		Auswirkung der Einschränkung wo wichtig	Erforderlich für den Unterricht?	Relevanz für die Sicherheit a) von personenbezogenen Daten b) der Schul IT Infrastruktur
Koppeln mit Apple Watch erlauben	▢		**Nein**	Am iPad irrelevant
Handgelenkerkennung bei Apple Watch erzwingen	▢		**Nein**	s.o.
Ändern von Bluetooth-Einstellungen (einschließlich Kopplung neuer Geräte) erlauben	☑		**Ja**, um das Koppeln von Geräten wie Drohnen, Robotern, Stiften, Tastaturen und ähnlich zu ermöglichen. Bezug zu MKR 6.3	Geringe Relevanz
Geräten nur den Beitritt zu WLAN-Netzwerken erlauben, die mit einem Profil konfiguriert wurden	☑		**Ja**, um die Nutzung von sicheren WLAN-Netzwerken zu gewährleisten.	a) Relevant, da personenbezogene Daten übertragen werden können

WLAN durchgehend aktiviert lassen	☑		**Ja,** um die WLAN-Funktion ständig aktiviert zu halten	b) Geräte müssen für das MDM erreichbar bleiben.
Erstellen von VPN-Konfigurationen erlauben	▢		Ja, um sichere Verbindungen zu ermöglichen Auf Koffergeräten nicht relevant.	a) Relevant, da personenbezogene Daten übertragen werden können

Benutzeranpassungen

Payload		Auswirkung der Einschränkung wo wichtig	Erforderlich für den Unterricht?	Relevanz für die Sicherheit a) von personenbezogenen Daten b) der Schul IT Infrastruktur
Ändern der Accounteinstellungen (E-Mail, Kontakte, Kalender, iCloud und iTunes Store)	▢		**Nein**	a) Relevant, da damit auf persönliche Informationen zugegriffen werden kann, wenn Schüler sich mit privater Apple ID anmelden und nicht abmelden
Verwenden der Einstellung "Alle Inhalte & Einstellungen löschen" erlauben	▢		**Nein**, da es sich nicht um Geräte handelt, die nur eine Person benutzt. Für die Einhaltung von Löschfristen ist die Lehrperson zuständig.	a) Relevant, da dadurch alle persönlichen Daten gelöscht werden können, die vorübergehenden auf einem Gerät gespeichert werden sollen
Ändern der Einstellungen für „Freunde suchen“ erlauben	▢		**Nein**	a) Bedingt relevant, da damit auf persönliche Informationen zugegriffen werden kann

Installation von Konfigurationsprofilen erlauben	▢		**Nein**	b) Über Konfigurationsprofile könnten Einschränkungen durch die Schule beeinflusst werden
Ändern des Gerätenamens erlauben	▢	Diese Einstellung verhindert, wenn aktiviert, auch, dass das MDM-Profil den Namen des überwachten Geräts ändert. Wenn diese Einstellung deaktiviert ist, kann ein Administrator ein überwachtes Gerät nicht aus der Ferne festlegen oder automatisch benennen.	**Nein**, bei unpersonalisierten Geräten nicht erforderlich	a) Nicht relevant für die Sicherheit von personenbezogenen Daten b) kann zu falscher Identifizierung von Geräten führen.
Tastaturkurzbefehle erlauben	☑		**Ja**	a) Nicht relevant für die Sicherheit von personenbezogenen Daten
App-Installation über den App Store erlauben	▢		**Nein**, bei Koffergeräten nicht relevant.	b) Relevant, da dadurch möglicherweise unsichere oder bösartige Apps installiert werden können
Ändern persönlicher Hotspots erlauben	▢		**Nein**	a) Relevant, da damit auf persönliche Informationen zugegriffen werden kann
Entfernen von Rapid Security Response erlauben	▢		**Nein**	b) Relevant, da dadurch möglicherweise die Sicherheit des Geräts beeinträchtigt werden kann
Benutzer das Ändern des Hintergrundbilds erlauben	▢		**Nein**, bei unpersonalisierten Geräten nicht erforderlich	a) Nicht relevant für die Sicherheit von personenbezogenen Daten
Ändern von Mitteilungseinstellungen erlauben	▢		**Nein**	a) Relevant, da damit auf persönliche Informationen zugegriffen werden kann

Einrichten neuer Geräte in der Nähe erlauben	▢		**Nein**	Keine Relevanz
Hinzufügen oder Entfernen einer Mobilfunkverbindung erlauben	▢		**Nein**	Keine Relevanz
Ändern von Einstellungen für Mobilfunkverbindungen für Apps erlauben	▢		**Nein**	Keine Relevanz
Ändern von Mobilfunkverbindungen erlauben	▢		**Nein**	Keine Relevanz
Continuous Path Tastatur erlauben	▢		**Nein**	a) Nicht relevant für die Sicherheit von personenbezogenen Daten
Automatisches Einstellen von Datum und Uhrzeit erzwingen	☑		**Ja**	b) Relevant, da damit die Sicherheitseinstellungen des Geräts verbessert werden können
Anzeigen von App-Clips erlauben	▢		**Nein**	a) Nicht relevant für die Sicherheit von personenbezogenen Daten

Anmerkungen

Pädagogisch didaktische Erfordernisse (nach dem Medienkompetenzrahmen NRW, kurz MKR)

1.3 Datenorganisation

Die Schülerinnen und Schüler sollen…

Informationen und Daten sicher speichern, wiederfinden und von verschiedenen Orten abrufen;
Informationen und Daten zusammenfassen, organisieren und strukturiert aufbewahren

Umsetzung auf dem iPad:

- Speichermöglichkeit und Datenorganisation in der Dateien App
- datenschutzkonforme Cloud-Lösung mit Einbindung in das Apple-Dateisystem (ein Cloud-Zugang nur über den Browser ist nicht praktikabel)

1.4 Datenschutz und Informationssicherheit

Die Schülerinnen und Schüler sollen…

Verantwortungsvoll mit persönlichen und fremden Daten umgehen;
Datenschutz, Privatsphäre und Informationssicherheit beachten

Umsetzung auf dem iPad:

- Ein Bewusstsein schaffen, dass im Internet keine persönlichen Daten hinterlassen werden sollten. Es sei denn, es handelt sich um vertrauenswürdige Seiten, die von den Lehrkräften genannt werden (z. B. Logineo LMS oder Mail4Kidz).

2.1 Informationsrecherche

Die Schülerinnen und Schüler sollen…

Informationsrecherchen zielgerichtet durchführen und dabei Suchstrategien anwenden

Umsetzung auf dem iPad:

- Informationen müssen auffindbar sein. Filter dürfen nicht so restriktiv eingestellt sein, dass sie nur wenige Seiten durchlassen
- Safari oder alternative Browser müssen verfügbar sein
- Für Schülerinnen und Schüler mit zusätzlichem Unterstützungsbedarf kann die Suche über Siri (Suchbegriffe werden gesprochen) angeboten werden

3.1 Kommunikations- und Kooperationsprozesse

Die Schülerinnen und Schüler sollen…

Kommunikations- und Kooperationsprozesse mit digitalen Werkzeugen zielgerichtet gestalten sowie mediale Produkte und Informationen teilen

Umsetzung auf dem iPad:

- Teilen über AirDrop ermöglichen und/oder
- über eine digitale Pinnwand
- einen sicheren Messenger
- oder ein Lernmanagement System

4.1 Medienproduktion und Präsentation

Die Schülerinnen und Schüler sollen…

Medienprodukte adressatengerecht planen, gestalten und präsentieren; Möglichkeiten des Veröffentlichens und Teilens kennen und nutzen

Umsetzung auf dem iPad:

- Teilen über AirDrop und/oder eine Cloud, die im Dateisystem des iPad eingebunden ist
- Präsentation über AirPlay und/oder eine digitale Pinnwand oder ein Lernmanagement System
- Möglichkeit des Druckens

4.2 Gestaltungsmittel

Die Schülerinnen und Schüler sollen…

Gestaltungsmittel von Medienprodukten kennen, reflektiert anwenden sowie hinsichtlich ihrer Qualität, Wirkung und Aussageabsicht beurteilen

Umsetzung auf dem iPad:

- Die Schule muss die Freiheit haben, verschiedene Apps auswählen zu dürfen, die für den Unterricht geeignet sind (z. B. Book Creator, Sketches School etc.)
- Die Schule muss die Freiheit haben, bestimmte Eingabemethoden anbieten zu können (z. B. Arbeiten mit einem digitalen Stift, mit Spracheingabe und/oder mit einer Tastatur)

4.4 Rechtliche Grundlagen

Die Schülerinnen und Schüler sollen…

Rechtliche Grundlagen des Persönlichkeits- (u.a. des Bildrechts), Urheber- und Nutzungsrechts (u.a. Lizenzen) überprüfen, bewerten und beachten

Umsetzung auf dem iPad:

- Schülerinnen und Schülern wird das Recht gewährt, eigene Inhalte löschen zu dürfen (auf dem Gerät und in der Cloud)

5.4 Selbstregulierte Mediennutzung

Die Schülerinnen und Schüler sollen…

Medien und ihre Wirkungen beschreiben, kritisch reflektieren und deren Nutzung selbstverantwortlich regulieren; andere bei ihrer Mediennutzung unterstützen

Umsetzung auf dem iPad:

- Apps werden nicht unangekündigt zeitlich beschränkt bzw. gesperrt oder entfernt (vgl. auch Anmerkungen zu Punkt 2.1)
- Die Aktivitäten von Schülerinnen und Schülern werden nicht ohne Ankündigung bzw. Begründung beobachtet (z. B. über die Classroom App)

6.3 Modellieren und Programmieren

Die Schülerinnen und Schüler sollen…

Probleme formalisiert beschreiben, Problemlösestrategien entwickeln und dazu eine strukturierte, algorithmische Sequenz planen; diese auch durch Programmieren umsetzen und die gefundene Lösungsstrategie beurteilen

Umsetzung auf dem iPad:

- Zusätzliche Hardware, die für die Umsetzung von Lerninhalten im Unterricht notwendig ist, muss über Bluetooth gekoppelt werden können (z. B. Bluebots, Tastaturen etc.)

Weitere Informationen rund um das Thema Einsatz von Endgeräten und Datenschutz

- https://www.schulministerium.nrw/fragen-und-antworten-zur-ausstattung-von-schuelerinnen-und-schueler-sofortausstattungsprogramm
- https://www.schulministerium.nrw/fragen-und-antworten-zum-datenschutz
- https://www.ldi.nrw.de/system/files/media/document/file/ldi_nrw_-_digitaler_unterricht_in_schulen_2022-10-25.pdf
- https://www.medienberatung.schulministerium.nrw.de/Medienberatung/Datensicherheit-und-Datenschutz/Datenschutzbeauftragte/

Die Player und ihre Perspektiven und Ansprüche

Schulträger

- Administration
- Support
- Standardisierung
- Minimierung Aufwand
- Beschaffung von Apps
- Installation von Apps
- Sicherheit Nutzer
- Sicherheit Infrastruktur
- Schutz der Hardware
- Schutz der Konfiguration
- Firewall/ Internetfilter

Lehrkräfte

- Umsetzung des pädagogischen Teils des schulischen Medienkonzeptes (Medienkompetenzrahmen NRW)
- unterrichtliche Nutzbarkeit
- erforderliche Funktionen von iOS
- minimale Einschränkungen
- Deaktivierung nicht benötigter/ störender Funktionen
- eigenständige Installation von Apps
- Angepasste Layouts
- Verteilen von Inhalten, z.B. via Airdrop
- Speichern von Lernartefakten der Schülerinnen und Schüler
- Classroom (Steuerung und Kontrolle)
- Löschung von Inhalten von iPads
- Konnektivität zu anderer Hardware (z.B. Bluetooth)
- Grundschulschriften installiert
- angepasste Einstellungen und Layouts je nach Klassenstufe
- keine für Funktionen erforderlichen Ports in Firewall blockiert

Die Schulleitung

- Verantwortlicher Datenverarbeitung
- Lehrkräften bei der Erfüllung des Bildungs- und Erziehungsauftrags unterstützen.

Datenschutzbeauftragte(r)

- Datenschutz

- Sicherheit der Verarbeitung
- DS-GVO Konformität
- Einhaltung schuldatenschutzrechtlicher Vorgaben

Hinweise zum Dokument

Bitte beachten Sie, dass dieses Dokument eine Empfehlung darstellt. Sie wurde unter Beteiligung von anderen am Thema interessierten Personen erstellt, die Inhalte beisteuerten, Anregungen gaben und Vorschläge für Payloads kritisch hinterfragen.

Versionshinweise

2023-05-24 - Ergänzung von Lizenzhinweisen - Version 1.02.