

**«Bring your own device» bei Mitarbeitenden der Schule – was es zu beachten gilt**

**Umsetzungsinstrument im ict-coach**

## Dokumenten-Informationen

Handlungsfeld: Arbeitsgeräte

Format: Information
Thema: zu beachten bei BYOD von Lehrpersonen

Dokumenten-ID: https://ict-2022.ch; UI-AG-BYOD MA

Version: UI-AG-2022-V1.0

**«Bring your own device» bei Mitarbeitenden der Schule – was es zu beachten gilt**

**Inhalte und Hintergründe**

Private Arbeitsgeräte werden von Mitarbeitenden der Schule meist als Zweitgeräte als Ergänzung zum Schulgerät und seltener als Hauptgerät in der Schule genutzt. Sobald ein privates Gerät durch einen Mitarbeitenden im Schulkontext genutzt wird, braucht es besondere Regelungen dazu. Eine Zusammenstellung, was es zu beachten gilt, ist hier aufgeführt. Diese Zusammenstellung ist nicht abschliessend und soll als Grundlage für eine vertiefte Bearbeitung des Themas durch die Schule dienen.

**Verwendung der Vorlage**

Die Schule Musterhausen nutzt diese Informationen als Grundlage für Gespräche mit dem externen 3rd Level-Support sowie dem Informationssicherheitsverantwortlichen der Schule, um eine bestmögliche Integration von privaten Geräten der Schulmitarbeitenden unter Berücksichtigung des Datenschutzes zu gewährleisten.

**Weiterführende Links**

Die aufgeführten Links verweisen auf Webseiten oder Dokumente, die einen Bezug zu diesem Umsetzungsinstrument aufweisen.

* ….
* ….
* ….

**Grundsätzliche Überlegungen zu BYOD für Mitarbeitende an Schulen**

BYOD für Mitarbeitende kann sowohl auf Seiten der Schule als auch auf Seiten der Mitarbeitenden Vor- und Nachteile bringen. In diesem Dokument werden zentrale Aspekte aufgeführt, die zu klären sind, wenn BYOD für Mitarbeitende eingeführt oder erlaubt werden soll.

Aufgrund der rechtlichen Fallstricke ist die Verwendung von BYOD bzw. privaten Arbeitsgeräten zu Unterrichtszwecken sowie für organisatorisch-administrative Aufgaben für Mitarbeitende der Schule spezifisch zu regeln. Nachfolgend eine Liste von Punkten, die üblicherweise in BYOD-Regelungen enthalten sind bzw. welche eine Schule zu klären hat. Gewisse Punkte sind in ihrer Umsetzung komplex. Es macht daher Sinn, diese in einem Gespräch mit den Mitarbeitenden zu thematisieren.

Diese Ausführungen verfolgen zwei Ziele: Erstens, das Risiko des Verlustes von Schuldaten zu minimieren und zweitens, dem Schutz der Schuldaten Rechnung zu tragen. Des Weiteren soll daran erinnert werden, dass mit der Umsetzung der Regeln Risiken insgesamt minimiert, aber nicht ausgeschlossen werden können.

**Grundsätzliches:**

**Freiwilligkeit**: Lehrpersonen sowie weitere Mitarbeitende können grundsätzlich nicht zur Teilnahme am BYOD-Modell verpflichtet werden. Umgekehrt haben Lehrpersonen und weitere Mitarbeitende, rechtlich gesehen, auch kein Recht auf BYOD. Die Schulen haben somit die notwendigen Arbeitsgeräte zur Verfügung zu stellen Es ist sinnvoll, ein Konzept zu erstellen, für welche Mitarbeitenden (bspw. Pensen abhängig) welche Nutzungsmodelle vorgesehen sind. Zudem ist zu regeln, wie viel Vorankündigungszeit die Schule für einen Wechsel zu oder weg von BYOD vorsieht.

**Kostentragung**:

Bei BYOD kaufen die Mitarbeitenden ihr Gerät selbst. Die Schule entscheidet, ob und in welcher Form sie den Mitarbeitenden eine Entschädigung zahlt (monatlich, halbjährlich oder einmalig). Weiter muss geklärt werden, wer für allfällige Reparaturkosten am Gerät aufkommen muss. Grundsätzlich gilt: Das Gerät bleibt in Privatbesitz und muss für die Arbeit an der Schule funktionstüchtig sein. Die für den Unterricht und die Schulorganisation genutzte Software inkl. Lizenzen werden den Mitarbeitenden von der Schule zur Verfügung gestellt. Die Nutzungsrechte an der Software verfallen mit dem Austritt. Der Benutzer wird verpflichtet, die Software zu deinstallieren

Die Schule kann Minimalstandards für BYOD-Geräte vorgeben, z.B., dass die Lehrpersonen, Schülerinnen und Schüler mit der gleichen Gerätekategorie arbeiten.

**Haftung**: Einerseits ist eineHaftung der Schule für private Geräte der Lehrpersonen und weiterer Mitarbeitenden denkbar. Andererseits können Lehrpersonen und weitere Mitarbeitende für Schäden, die durch ihre Arbeitsgeräte an der Basisinfrastruktur verursacht werden, verantwortlich gemacht werden, beispielsweise, wenn sie über ein solches Gerät das Netzwerk der Schule mit Malware infizieren. Spezifische Nutzungsregeln sowie eine vorgängige Bekanntgabe dieser Regeln sind wichtig und können bei einem Schaden unter Umständen sogar haftungsverschärfend wirken. Die Durchsetzung möglicher Ansprüche aus einer Haftung kann schwierig und aufwendig sein. Deshalb sollendie Parteien gemeinsam eine Lösung für einen entstandenen Schaden suchen.

**Datenschutz**: Eine grosse Herausforderung bei BYOD ist die datenschutzrechtskonforme Ausgestaltung. Die Daten auf den privaten Geräten der Nutzerinnen und Nutzer sind als Personendaten im Sinne des Datenschutzrechts zu qualifizieren.
Beispiel: Es braucht eine klare Trennung von rein privaten sowie «schulischen» Daten. Es bedarf einer Regelung, wie die schulischen Daten vor Diebstahl oder Verlust geschützt werden und der Verpflichtung der Mitarbeitenden, diese Regelung einzuhalten.

**Umsetzung:**

Vor dem Einsatz privater Geräte der Lehrpersonen und weiterer Mitarbeitenden sind folgende Punkte zu klären sowie folgende Prozesse oder Regelungen zu erarbeiten:

|  |
| --- |
| * Wie ist die grundsätzliche Haltung der Behörde und des Kollegiums gegenüber dem Einsatz privater Geräte der Mitarbeitenden an der Schule? Die Umsetzungsvarianten können von einem Verbot, über punktuelle oder vollständige Erlaubnis des Einsatzes privater Geräte der Mitarbeitenden gehen. Findet die Kostenbeteiligung der Schule am privaten Gerät einmalig oder periodisch statt?
 |
| * Es bedarf einer Regelung über die Erwartung an die Nutzerinnen und Nutzer. Diese beinhaltet, dass …
	+ sie sich für eine von der Schule vorgegebene Mindestlaufzeit für das BYOD-Modell entscheiden. Der Wechsel auf ein anderes Modell ist der Schule mit einer festgelegten Vorlaufzeit anzukündigen.
	+ das BYOD-Gerät der Mitarbeitenden exklusiv durch sie genutzt wird, d.h., dass ein Teilen des Geräts im privaten Bereich nicht erlaubt ist.
	+ das Gerät mit einem starken Passwort geschützt ist.
	+ das Gerät funktionsfähig und mit dem aktuellen Betriebssystem und Virenscanprogramm ausgestattet ist.
	+ geklärt ist, wer welchen Anteil der Reparaturkosten übernimmt.
	+ sie mit reduzierten technischen Supportleistungen der Schule einverstanden sind (Umfang ist festzulegen) und, falls nötig, mit schulischen Ersatzgeräten arbeiten.
 |
| * Eine technische Lösung für die Trennung von schulischen und privaten Daten ist eine Voraussetzung für den Einsatz des BYOD-Modells. Idealerweise ist dazu ein eigenes Laufwerk anzulegen, welches durch ein separates Passwort geschützt wird. Es ist ebenfalls zwischen Daten der Schulverwaltung und Lerndaten wie Aufgaben, Lösungen etc. zu unterscheiden.
 |
| * Zusätzlich hat die Speicherung personensensitiver Daten und besondere Personendaten auf den privaten Geräten im Zusammenhang mit BYOD eine besondere Bedeutung. Die Schule muss festlegen, wo und mittels welcher Laufwerke oder Cloud-Dienste diese Daten gespeichert werden sollen und wie auf diese zugegriffen werden kann (Bsp. VPN, VDI, RDS, Sync Clients). Wenn personensensitive Daten mit dem persönlichen Gerät synchronisiert werden, müssen die Mitarbeitenden sicherstellen, dass das Gerät exklusiv durch sie genutzt wird und nicht durch weitere Personen aus dem privaten Kreis. Zudem ist eine Bitlocker-Verschlüsselung oder eine äquivalente Verschlüsselung zwingend zu nutzen. Eine Remote-Access-Lösung ist standardmässig mit einer Zwei-Faktor-Authentifizierung einzurichten.

Eine Sensibilisierung und ein Kompetenzaufbau bezüglich des Datenschutzes im Zusammenhang mit BYOD soll fortlaufend individuell und im Kollegium stattfinden.* Bei der Nutzung des Geräts ist jederzeit die Geheimnispflicht und die Vertraulichkeit zu gewährleisten. Das Verwenden von Privacy Folien auf dem Bildschirm sowie das Sperren des Bildschirms beim Verlassen des Geräts sind hier zweckdienliche Möglichkeiten.
 |
| * Es sind Bestimmungen über die Aufbewahrung und Mindeststandards von Passwörtern zu erstellen und umzusetzen.
* Die Datensicherung muss bezüglich der Häufigkeit als auch bezogen auf das Speichermedium geregelt werden. Es empfiehlt sich eine zentrale Sicherung und geschützte Aufbewahrung zu ermöglichen.
 |
| * Es braucht eine Vereinbarung, die den Zugriff durch die Schule auf die schulrelevanten Daten auf den privaten Geräten regelt. Darin soll der Prozess der Fernwartung, falls dies vorgesehen ist, festgelegt werden wie auch das Vorgehen beim Einzug des Gerätes beispielsweise zur Geräteüberprüfung. Weiter ist auch darauf hinzuweisen, dass die Möglichkeit besteht, dass durch den Support der Schule Datenverluste auch bei privaten Daten entstehen könnte. Falls zur Überprüfung der lokalen Sicherheit auf dem BYOD-Gerät durch den Arbeitgeber Analysen oder Auswertungen erfolgen sollen, ist dies ebenfalls vorab zu vereinbaren.
 |
| * Welche Software soll verpflichtend sein? Wer ist an diesem Entscheidungsprozess beteiligt? Programme, die installiert werden, sollen ausschliesslich aus offiziellen und autorisierten resp. vertrauenswürdigen Quellen stammen. Für obligatorische Applikationen stellt die Schule eine Lizenz zur Verfügung.
 |
| * Bei Verlust, Diebstahl, Beschädigung, Befall mit Schadsoftware des Gerätes oder (vermutetem) unbefugtem Zugriff auf das Gerät braucht es einen definierten Meldeprozess.

Das Verbot der Vornahme nicht autorisierter Änderung an der Hardware oder am Betriebssystem («Jailbreak»/«Rooten» des Geräts) ist festzuhalten. Der Prozess zum Schutz vor Viren bei den persönlichen Geräten sowie der Schul-ICT-Infrastruktur ist zu definieren.Es empfiehlt sich eine Nutzungsvereinbarung durch die Mitarbeitenden unterzeichnen zu lassen, welche im Personaldossier abgelegt wird. Eine Vorlage dazu findet sich im ICT-Coach bei den [Umsetzungsinstrumenten unter Arbeitsgeräte](https://ict-coach.ch/zh/site/assets/files/1218/ui-nutzungsregelung_lehrpersonen_byod.docx). |

Impressum

Autorenteam: Mitarbeitende der Fachstelle Bildung und ICT

Herausgeber: Bildungsdirektion Kanton Zürich
Volksschulamt
Abt. Pädagogisches
Fachstelle Bildung und ICT

Kontakt: edu-ict@vsa.zh.ch

Dokumenten-ID: https://ict-2022.ch; UI-AG-BYOD MA

Version: V-2022-001

Dieses Umsetzungsinstrument kann unter Einhaltung der [CC-Lizenz 4.0](https://creativecommons.org/licenses/by/4.0/legalcode.de): CC-BY genutzt werden.

Bildungsdirektion Kanton Zürich

Volksschulamt

