



KREISSCHULE

Aarau-Buchs

Technisches ICT-Konzept 2020+

Kreisschule Aarau-Buchs

Dokumentenkontrolle

Autor(en):	Netree AG, Patrick Füg / Daniel Buehlmann
Status:	Finale Version des Auftragnehmers – zur Freigabe durch den Kunden
Klassifizierung:	Vertraulich / nicht öffentlich
Ablage:	Beim Kunden
Erstellt mit:	Microsoft Word Office 365
Verteiler:	Kreisschule Aarau-Buchs: Bürgi Remi, Frey Helene, Streit Peter, Nunziata Salvatore

Änderungskontrolle

Version	Aktion	Datum	Autor(en)
001	Initial Version	24.09.2019	FUE
002	Inhaltsverzeichnis und Framework, adaptiert aus den ersten zwei Workshops.	27.11.2019	FUE
003	Detailinformationen aus den verschiedenen Workshops.	09.01.2020	FUE
004	Weiterführung, pädagogische Szenarien	13.01.2020	FUE
005-019	Konzeptarbeit weiterführen	14.01.-06.02.2020	FUE/BUE
020	Konzept finalisieren	07.02.2020	FUE
021	Kapitel Review – Hinweise und Entscheidungen zu den Kapiteln	12.02.2020	FUE
022	Anpassungen bei Optionen	25.05.2020	PST
023	Bearbeitung für Vernehmlassung	10.05.2021	PST

Inhaltsverzeichnis

1. Einleitung	2
1.1 Stellenwert	2
1.2 Zweck	2
2. Ausgangslage	2
2.1 Bedeutung und Zielsetzung	2
2.2 Handreichung BKS	3
2.3 Gesetzliche Grundlagen	3
2.4 Pädagogische Szenarien (Use-Cases)	4
2.4.1 Zyklus 1	4
2.4.2 Zyklus 2	4
2.4.3 Zyklus 3	5
2.4.4 Zyklusübergreifend	6
2.4.5 Home	7
2.5 Geräteausstattung	7
2.5.1 Berechnung Anzahl Geräte SuS	8
2.5.2 Berechnung Anzahl Geräte LP	10
2.5.3 Berechnung Dockingstation und Aufbewahrung	11
2.5.4 Verwendung privater Geräte [BYOD]	12
2.6 Formfaktor und Betriebssystem	13
2.6.1 Lebensdauer	14
2.6.2 Ausstattung SuS	15
2.6.3 Ausstattung LP	16
2.6.4 Erläuterungen	17
2.7 Rahmenbedingungen	17
2.7.1 Professionelle Infrastruktur in den Schulen	17
2.7.2 Umgang mit Apps, Software und Fachanwendungen	18
2.7.3 Netzwerk	18
2.7.4 Datenschutz bei Cloud-Diensten	18
2.7.5 Cloud & Plattformen	20
2.7.6 Umsetzung ICT-Konzept 2020+	20
2.8 IST-Analyse	20
2.8.1 Endgeräte	21
2.8.2 Peripherie	22
2.8.3 Netzwerk	22
3. Lösungsansatz	23
3.1 Architektur	24
3.2 Infrastruktur-Services	25
3.2.1 Benutzer-Identität	25
3.2.2 Printing	26
3.2.3 Microsoft Office 365	27
3.2.4 Microsoft Intune (MDM-Lösung)	28
3.2.5 Erweiterte Sicherheit (Advanced Security)	29

3.2.6 Datenschutz und Datenablage (File Ablage).....	30
3.2.7 Managed Device.....	31
3.3 Voraussetzungen Netzwerk.....	32
4. Betrieb und Support.....	34
4.1 Organisation.....	35
4.2 Steuerung und Support.....	35
4.3 Kalkulatorischer Aufwand PICTS.....	39
4.3.1 Entschädigungsmodell pro Endgerät.....	39
4.3.2 Empfehlung.....	39
4.4 Berechnungsgrundlagen Betrieb und Support (extern).....	40
4.4.1 Modell pro Endgerät.....	41
4.4.2 Zusammenfassung der Berechnung.....	42
4.4.3 Empfehlung.....	42
4.4.4 Gegenüberstellung IST-SOLL (Konzept).....	42
4.5 SLA.....	43
5. Datensicherheit und Datenschutz.....	45
6. Gesamtkostenbetrachtung (TCO – 5 Jahre).....	46
6.1 Berechnung TCO.....	48
7. Anhang.....	49
7.1 Tabellenverzeichnis.....	49
7.2 Abbildungsverzeichnis.....	50
7.3 Softwareverzeichnis (Schul- und Fachapplikationen).....	Fehler! Textmarke nicht definiert.
7.3.1 SOLL-Zustand.....	Fehler! Textmarke nicht definiert.
7.3.2 IST-Zustand.....	Fehler! Textmarke nicht definiert.
7.4 Microsoft Lizenzierung.....	Fehler! Textmarke nicht definiert.
7.5 Microsoft Office 365 CH-Datacenter.....	Fehler! Textmarke nicht definiert.
7.6 Microsoft Office 365 Datensicherung.....	Fehler! Textmarke nicht definiert.
7.7 Microsoft Office 365 Cloud to Cloud Backup.....	Fehler! Textmarke nicht definiert.
7.8 Apple / MDM Microsoft Intune.....	Fehler! Textmarke nicht definiert.
7.9 Unterscheidung päd. – techn. – Support.....	Fehler! Textmarke nicht definiert.
8. Stichwortverzeichnis.....	51

1. Einleitung

1.1 Stellenwert

Kinder und Jugendliche wachsen in einer Welt auf, die von elektronischen Medien durchdrungen ist. Diese digitale Welt ist allgegenwärtig und bestimmt unser Verhalten in der privaten Umgebung und in der Arbeitswelt. Die Schule leistet dabei einen Beitrag, die Schülerinnen und Schüler auf ein Leben mit digitalen Medien vorzubereiten. Dazu gehört die Kompetenz, in dieser vernetzten Welt und der Informationsgesellschaft sachgerecht, kreativ und mündig zu leben und sich sozial verantwortlich und selbstbestimmt zu verhalten.

1.2 Zweck

Das technische ICT-Konzept 2020+

- beschreibt die Mittel, welche für die Erreichung der Ziele notwendig sind und definiert die Ressourcen für einen zeitgemässen ICT- und Medieneinsatz;
- weist auf der Grundlage einer definierten Standardausrüstung die Kosten aus;
- stellt sicher, dass für die Umsetzung im Unterricht ausreichende, adäquate und dem Standard entsprechende Hard- und Software zur Verfügung steht;
- erlaubt den Schülerinnen und Schülern sowie Lehrpersonen den selbständigen, sich aus dem aktuellen Lernprozess heraus ergebenden Einsatz von ICT-Mitteln im Unterricht;
- leitet verantwortliche Stellen und Gremien wie Kreisschulrat, Kreisschulpflege und Schulleitung in ihren zukünftigen Entscheidungen.

2. Ausgangslage

2.1 Bedeutung und Zielsetzung

Eine zeitgemässe und moderne ICT-Ausstattung und Konzeption soll auf Basis der verschiedenen Anforderungen und Bedürfnissen der Kreisschule Aarau-Buchs verarbeitet werden.

Als technischen Zielsetzungen sollen erreicht werden:

- eine für den ICT-Betrieb optimierte Lösung
- minimaler eigener Infrastruktur und tendenziell in der Cloud
- vollumfängliche Erfüllung der Anforderungen aus dem Lehrplan 21
- Abgrenzungen in den Services

Zu berücksichtigen ist die aktuelle Situation und Ausstattung der Schulen. Wenn möglich sollen Teile davon in der Konzeption und späteren Ausstattung berücksichtigt werden. Konkret sind dies bereits beschaffte Gerätschaften (verschiedene Endgeräte) und Ausrüstungen für den informatischen Schulunterricht (Medien & Informatik).

2.2 Handreichung BKS

Das Departement Bildung, Kultur und Sport (BKS) stellt seit 19. Februar 2019 eine Handreichung «Informations- und Kommunikationstechnologie (ICT) an der Volksschule» zur Verfügung. Diese zeigt Rahmenbedingungen und Aspekte auf, die sich rund um die Einführung des Aargauer Lehrplans Volksschule mit dem Modul «Medien und Informatik» stellen und bietet für Schulen die Chance, sich vertieft mit Fragen zur Ausstattung, Nutzung und Wirkung digitaler Technologien auseinanderzusetzen. Sie gibt Empfehlungen ab zur Erstellung von Medien- und Informatikkonzepten, zur Planung von Support-Leistungen und zur schulischen Infrastruktur. Zudem wird aufgezeigt, worauf beim Umgang mit digitalen Daten zu achten ist, um die Umsetzung der Datensicherheit zu gewährleisten, und wo weiterführende Informationen und Unterstützungsangebote zum Themenbereich Medien und Informatik zu finden sind. Handreichung des Departements BKS vom 23. September 2019

2.3 Gesetzliche Grundlagen

Der neue Aargauer Lehrplan Volksschule gilt ab 1. August 2020. Er basiert auf dem Deutschschweizer Lehrplan («Lehrplan 21») und beinhaltet das Modul «Medien und Informatik».

Grundlagen

- Gestützt auf §13 des Schulgesetzes legt der Regierungsrat nach Anhörung des Erziehungsrates die einzelnen Unterrichtsfächer, die Zahl der Unterrichtslektionen und ihre Dauer sowie Lernziele und die Stoffauswahl fest.
- Gemäss § 53 des Schulgesetzes beschaffen und unterhalten die Gemeinden das Mobiliar, die Schuleinrichtungen und die Lehrmittel.

Verantwortlichkeiten

- Damit ist die Gemeinde für die Ausrüstung im Informatik-Unterricht verantwortlich und stellt die notwendige Hard- und Software sowie Netzwerke und Datenablage sicher.
- Ebenso fällt der technische Support in die Zuständigkeit der Gemeinde.
- Bezüglich Weiterbildung existieren Angebote der FHNW, die Nutzung und Finanzierung fällt wiederum in die Verantwortung der Gemeinde.

2.4 Pädagogische Szenarien (Use-Cases)

In den nachfolgenden Szenarien soll eruiert werden, wie beispielsweise mit einer Cloud-/Schulplattform (Microsoft Office 365 Education) konkrete Unterrichtssequenzen (pädagogische Szenarien) umgesetzt werden. Sie beziehen sich alle auf den Lehrplan 21. Die Szenarien belegen Tendenzen in der Wahl und Ausstattung der Arbeitsmittel, sprich Endgerätewahl.

Zyklus	Stufe
Zyklus 1	Kindergarten bis 2. Klasse
Zyklus 2	Primarstufe 3.-6. Klasse
Zyklus 3	Sekundarstufe I (7.-9. Klasse)

Tabelle 1 Erläuterung der Zyklen

2.4.1 Zyklus 1

<i>Szenario 1</i>	Kinder im Kindergartenalter experimentieren kreativ und spielerisch in Kleingruppen mit speziell auf das Alter abgestimmten Apps. Dazu arbeiten sie in Kleingruppen mit 2-3 Tablets, die von der Schule bereitgestellt werden. Ein Login ist dafür nicht nötig.
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ Tablet (einfaches Handling, vertraut vom Smartphone) ✓ Betriebssystem: Abhängig vom Anbieter der App

<i>Szenario 2.Z1</i>	<p>In Phasen, bei welchen mit erweiterten Lehr- und Lernformen gearbeitet wird, üben einzelne SuS das Rechnen mit einer Lernsoftware (z. B. Blitzrechnen) oder einem interaktiven (digitalen) Arbeitsblatt.</p> <ul style="list-style-type: none"> ▪ Die individuellen Lernstände werden beim Abmelden userspezifisch gespeichert. ▪ Die Lehrperson kann die Arbeitsfortschritte kontrollieren
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ App-Spezifische Anforderungen ✓ Internetzugang bei cloudbasierter Anwendung (z.B. profaxonline) ✓ Bedingt eine Benutzer-Anmeldung

2.4.2 Zyklus 2

<i>Szenario 2.Z2</i>	<p>In Phasen, bei welchen mit erweiterten Lehr- und Lernformen gearbeitet wird, üben einzelne SuS das Rechnen mit einer Lernsoftware (z. B. Blitzrechnen) oder einem interaktiven (digitalen) Arbeitsblatt.</p> <ul style="list-style-type: none"> ▪ Die individuellen Lernstände werden beim Abmelden userspezifisch gespeichert. ▪ Die Lehrperson kann die Arbeitsfortschritte kontrollieren
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ App-Spezifische Anforderungen ✓ Internetzugang bei cloudbasierter Anwendung (z.B. profaxonline) ✓ Bedingt eine Benutzer-Anmeldung

<i>Szenario 3</i>	Die Klasse arbeitet intensiv mit einer browserbasierten Lernapplikation. Dazu benötigt jedes Kind ein Device. Neben den sich im Zimmer befindenden Geräten, werden die zusätzlich benötigten Geräte aus dem Pool im Materialzimmer geholt. Alle SuS können nach dem Anmelden an die webbasierte Plattform (per Browser) die benötigten Web-Apps benutzen.
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ Aktuelle webbasierte Applikationen können mit allen mobilen Geräten abgedeckt werden. ✓ Neben den auf die Schulzimmer zugewiesenen Geräte ist ein Schulhaus-Pool notwendig.

<i>Szenario 4</i>	Eine Klasse mit 25 SuS programmiert im Fach «Medien und Informatik» auf einer browserbasierten Onlineapplikation ein Game und erstellt anschließend in einem Textverarbeitungsprogramm eine Bedienungsanleitung und eine technische Dokumentation (siehe connected 2 [<i>integratives Lehrmittel für Medien und Informatik</i>], Kapitel 5K). Jeder Schüler hat ein eigenes Login mit Benutzername und Passwort und gibt über die Tastatur den Text ein.
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ Aktuelle webbasierte Applikationen können mit allen mobilen Geräten abgedeckt werden. ✓ Neben den auf die Schulzimmer zugewiesenen Geräte ist ein Schulhaus-Pool an Geräten mit einer Tastatur notwendig.

2.4.3 Zyklus 3

<i>Szenario 5</i>	Die Klasse arbeitet intensiv mit einer browserbasierten Lernapplikation. Dazu benötigt jedes Kind ein Device, welches es immer auf sich trägt. Alle SuS können nach dem Anmelden an die webbasierte Plattform (per Browser) die benötigten Web-Apps benutzen.
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ Persönliches SuS-Gerät ✓ Benutzer-Anmeldungen

<i>Szenario 6a</i>	<p>Die SuS arbeiten an einer Reportage im Klassenteams:</p> <ul style="list-style-type: none"> ▪ Durch das Login in die Schulplattform können die Bilder- und Tondateien einfach vom verwendeten Gerät in das Präsentationstool oder Datenablage importiert oder synchronisiert werden. ▪ Während den Bearbeitungssequenzen werden die grossen Ton- oder Filmdateien meistens gleichzeitig am Ende der Lektion gespeichert. Dazu wird die hohe Bandbreite der Internetverbindung sehr geschätzt. ▪ Aus den wesentlichen Aussagen wird ein kurzer Film oder eine Präsentation erstellt. Das Arbeitsergebnis kann der Klasse in geeigneter Weise direkt ab dem mobilen Gerät vorgeführt werden. Dazu sollen standardisierte drahtlose Übertragungen zum Beamer genutzt werden, um die unterschiedlichen Gerätetypen nutzen zu können. ▪ Produktion eines Audiofiles, das der Klasse vorgespielt wird. ▪ Präsentation der Ergebnisse im Klassenblog. ▪ Ausdrucken der fertigen Arbeit als Text- und Bilddokument. Es gibt in jedem Schulhaus die Möglichkeit zu drucken so lange man sich im Schul-WLAN eingeloggt hat. Egal von welchem Device aus dies gewünscht ist.
--------------------	--

	<ul style="list-style-type: none"> ▪ Speichern aller erarbeiteten Dokumente und Links im Klassenarbeitsraum.
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ Klassischer Kollaborations-Lern-Situation mit verschiedenen Endgeräten (Private Smartphones, Tablets und Schulgeräte). Kann vollumfänglich mit Office 365 (Microsoft Teams/SharePoint Online) abgedeckt werden.

<i>Szenario 6b</i>	<p>Eine Gruppe von SuS erhält den Auftrag zum Thema «Blut, Blutkreislauf» zu recherchieren. Sie erstellen einen Gruppenarbeitsraum und halten ihre Ergebnisse stichwortartig in einem gemeinsamen Mindmap fest. Sie präsentieren ihre Erkenntnisse der Klasse. Nach der Präsentation gibt es für die zuhörenden SuS noch ein Quiz (Multiple Choice) mit Fragen zum Präsentierten. Das Quiz hat das Team mit Hilfe einer Quiz-App erstellt. Die Fragen können auf geeignete Weise projiziert werden. Die ratenden SuS können ihre Antworten auf ihrem Tablet oder Handy eingeben. Die Auswertung erfolgt automatisch.</p>
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ Klassischer Kollaborations-Lern-Situation mit verschiedenen Endgeräten (Private Smartphones, Tablets und Schulgeräte). Kann vollumfänglich mit Office 365 (Microsoft Teams/SharePoint Online) abgedeckt werden.

2.4.4 Zyklusübergreifend

<i>Szenario 7</i>	<p>Begabtenförderung Thema «Roboter», die SuS programmieren mit einer produktespezifischen, lokal installierbaren Software einen Roboter aus einem Baukastensystem (z. B. Lego Mindstorms). Sie laden sich dazu auch neue Programmierbausteine aus dem Internet herunter.</p>
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ Der Pool könnte grundsätzlich mit allen mobilen Formfaktoren abgedeckt werden. Ausschlaggebend ist die technische Voraussetzung des elektronischen Lehrmittels, geforderten Schnittstellen und die Arbeitsweise.

<i>Szenario 8</i>	<p>Die Lehrperson einer Schule tauschen gegenseitig Beurteilungsberichte aus, indem sie sie auf einem gemeinsamen Share nach Fächern getrennt ablegen. Der Share ist nur für die Lehrpersonen des jeweiligen Schulhauses zugänglich. Die Vorlagen dazu können auf einem Share allen Lehrpersonen der Kreisschule zugänglich gemacht werden. Sie können die Berichte von irgendeinem Device aus online weiterbearbeiten.</p>
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ Ablegen von besonders schützenswerten Personendaten in der Cloud (Office 365) müssen zusätzlich verschlüsselt werden (Customer Key).

2.4.5 Home

<i>Szenario 9</i>	Schülerin X arbeitet auf dem privaten Notebook der Familie an den Hausaufgaben. Das Login ist gleich wie in der Schule über eine Webseite zugänglich. Es stehen die gleichen Apps wie in der Schule zur Verfügung. Mit Computer, Tablet oder Smartphone möglich. → Die SuS können zuhause mit privaten Geräten an der Stelle weiterarbeiten, wo sie in der Schule stehen geblieben sind.
<i>Fazit</i>	<ul style="list-style-type: none"> ✓ Office 365 ✓ weitere cloudbasierte Anwendungen (z.B. profaxonline) ✓ Bedingt Benutzer-Anmeldungen

2.5 *Geräteausstattung (Neubeurteilung nach Erarbeitung des pädagogischen ICT-Konzepts)*

Ziel und vorgesehen ist der Einsatz von mobilen Endgeräten (Tablet/Convertible/Notebook) im Unterricht für die Schüler*innen und Lehrpersonen. In der Primarschule sollen zusätzlich Pools an den einzelnen Schulstandorten eingesetzt werden, um die bestmögliche Abdeckung im Unterricht für die Lernenden zu erreichen.

Stufe	Geräte fix in der Klasse	Pool, für das ganze Schulhaus
Kindergarten	2 Tablets	-
1. bis 3. Klasse	Pro 3 SuS ein Tablet (3:1)	-
4. bis 6. Klasse	Pro 2 SuS ein Convertible (2:1)	25 Convertible
Sekundarstufe 1	1:1 Convertible	-

Stufe	Geräte fix in der Klasse	Pool, für das ganze Schulhaus
<i>Kindergarten</i>	<i>2 Tablets</i>	-
<i>1. & 2. Klasse</i>	<i>Pro 3 SuS ein Tablet (3:1)</i>	-
<i>3. bis 6. Klasse</i>	<i>Pro 2 SuS ein Convertible (2:1)</i>	<i>25 Convertible</i>
<i>Sekundarstufe 1</i>	<i>1:1 Convertible</i>	-

Tabelle 2 Stufe und Geräteausstattung

Begründung: Es hat sich gezeigt, dass sich die Aufteilung der Geräteausstattung in der Praxis nicht bewähren wird, da die Klassenlehrperson jeweils nach zwei Schuljahren wechseln wird und so ein Systemwechsel (Tablet zu Convertible) sinnvollerweise nach der zweiten und nicht nach der dritten Klasse erfolgen muss.

2.5.1 Berechnung Anzahl Geräte SuS

Berechnung Schuljahr 2019/2020

Kindergarten	Abteilungen	Ausstattung	Pool	Total Geräte
	30	2	0	60
Primarschule	Anzahl SuS	Faktor	Pool	Total
1. - 3. Klasse	840	0.333	0	279.72
Primarschule	Anzahl SuS	Faktor	Pool [Siehe ff. Tabelle 4]	Total
4. - 6. Klasse	760	0.5	117	497
Oberstufe	Anzahl SuS	Faktor		Total
	1120	1	20	1140
				Gesamt
				1977

Berechnung Schuljahr 2020/2021

Kindergarten	Abteilungen	Ausstattung	Pool	Total Geräte
	30	2	0	60
Primarschule	Anzahl SuS	Faktor	Pool	Total
1. & 2. Klasse	561	0.333	0	186.813
Primarschule	Anzahl SuS	Faktor	Pool	Total
3. - 6. Klasse	1075	0.5	117	654.5
Oberstufe	Anzahl SuS	Faktor		Total
	1160	1	20	1160
				Gesamt
				2081

Tabelle 3 Berechnung Anzahl Endgeräte SuS

Ergänzung: Die Kreisschulpflege spricht sich am 30. März 2020 für den folgenden Beschluss aus: Die Geräte für die Schüler/innen sind Eigentum der Schule und werden durch diese beschafft und gewartet.

<i>Aare</i>	<i>Gysimatte</i>	<i>Gönhard</i>	<i>Risiacher</i>	<i>Rohr</i>	<i>Schachen</i>	<i>Telli</i>
1	2	2	1	1	1	1
-	Gysimatte	Trakt 1-3	-	-	-	-
-	Altes Schulhaus	Trakt 4	-	-	-	-
<i>Total</i>	<i>Faktor</i>	<i>Anzahl</i>				
9	13	117				

Tabelle 4 Berechnung Endgeräte Primarschule im Pool

2.5.2 Berechnung Anzahl Geräte LP

Die Grundlage bildete eine aktuelle Erhebung der rund 500 Angestellten der Kreisschule Aarau-Buchs. Für die konzeptionelle Ausrichtung wird davon ausgegangen, dass alle Angestellte (Lehrpersonen) ab einem Anstellungsgrad ab 40% mit einem Endgerät ausgerüstet werden. Lehrpersonen mit einem geringeren Pensum (<40%) erhalten die Möglichkeit, Endgeräte aus dem **Standort-Pool** (1:3) zu nutzen oder das eigene, private Endgerät an der Schule (BYOD) einzusetzen.

Berechnung Schuljahr 2019/2020

Pensum		ab 40%	
Lehrpersonen alle	511	Geräte Total	387
Lehrpersonen über 40%	325	1:1	325
Lehrpersonen unter 40%	186	1:3	62

Tabelle 5 Berechnung Anzahl Endgeräte LP

Ergänzung: Eine Neuberechnung der Anzahl der Endgeräte für Lehrpersonen wird in der Ausarbeitung zur Erstellung der Dokumente für die Volksabstimmung erfolgen. Zu erwarten ist eine höhere Anzahl an Lehrpersonen, da die Schülerzahlen ebenfalls am Steigen sind.

BYOD (20% LP) und CYOD (80% LP) mit 2 Endgerätemodellen			
	Effektiv	Gesamt	
CYOD 1:1 (80%)	260		Persönliche Geräte
CYOD 1:3	62		LP-Pool, Shared Geräte
<i>BYOD (20%)</i>		65	<i>BYOD</i>
Total	322		Total (finanziert)
<i>Total</i>		387	<i>Total (alle LP)</i>

Tabelle 6 CYOD & BYOD

Aktualisierung: Neubeurteilung BYOD bei Lehrpersonen (siehe 2.5.4)

2.5.3 Berechnung Dockingstation und Aufbewahrung

Übersicht:

		Unterricht/ Vorbereitung	Klassen- zimmer	SuS- Pool	LP- Pool
Kindergarten	alle	30	-	-	-
Primarschulhaus	Aare	19	8	1	1
	Brunnbach	15	11	1	1
	Gönhard	40	17	2	1
	Gysimatte	27	12	2	1
	Risiacher	30	14	1	1
	Schachen	16	6	1	1
	Telli	25	10	1	1
Oberstufenschulhaus	Stock	17			1
	OSA	35			1
	Suhrenmatte	25			1
	Stäppli	15			1
	Zelgli	43			1
Musikschule	Aarau	32			
	Buchs-Rohr	14			
Dockingstations (in allen Räumen Unterricht / Vorbereitung)		383			
Aufbewahrung/Laden (PS&OS) / Total (in allen Klassenzimmern PS)			99		
(in allen Pools)			78		
Aufbewahrung/Laden (PS) / Total (für LP-Geräte 1:3)				9	7
Aufbewahrung/Laden (OS) (für SuS Ersatzgeräte und LP-Geräte 1:3)					5

Tabelle 7 Berechnung Docking-Station / Aufbewahrung

Dockingstation:

- In allen Räumen (Unterricht / Vorbereitung) gemäss Auflistung, soll **eine Dockingstation**, für die von der Schule zur Verfügung gestellten Endgeräte der Lehrpersonen einberechnet werden: Total **383 Stk.**

Aufbewahrung:

- LP-Pool: Für die **fünf** Standorte werden pro Standort **ein** Notebookwagen Typ 2 für die SuS Ersatzgeräte und LP-Geräte 1:3 einberechnet (ateCart 16S/ CHF 2500/Stk.) inkl. Schliesssystem und Rollen ohne zusätzliche Netzteile.
- Aufbewahrung Kindergarten: Die iPads werden über die mitgelieferten Kabel aufgeladen und es ist somit kein weiteres Mobiliar notwendig!
- Unterstufe 1. bis 4. Klasse, **44** Lade- und Synchronisierungs-Kabinett, für max. 10 Tablets (Kensington K67862EU / CHF 600/Stk.), inkl. Schliesssystem.
- Unterstufe 5. Bis 6. Klasse, **26** Notebookwagen Typ 1, für max. 12 Geräte mit einer Grösse von bis zu 14 Zoll (Kensington AC12 Ladegerät / CHF 1200/Stk.), inkl. Schliesssystem.

- Primarschule 9 24-er-Notebookwagen Typ 3 (ateCart 24S/ CHF 2700/Stk.) für den jeweiligen Pool mit je mindestens 18 Geräte (Kalkuliert: 13 plus 5 Ersatzgeräte) inkl. Schliesssystem und Rollen ohne zusätzliche Netzteile.
- Für die 1:3 LP-Geräte in den sieben Primarschulhäusern ist eine Aufbewahrung mit Ladefunktion vorgesehen, für maximal 8 Geräte. Dazu eignen sich 7 Desktop-Ladeschränke (Ergotron Zip12 / CHF 900/Stk.).

Ausnahme:

- Oberstufe: Alle SuS (im 1:1) müssen zu Hause/Privat die Geräte laden und erhalten das mitgelieferte Netzteil mit, somit ist kein weiteres Mobiliar notwendig!

Hinweise:

- Die abschliessende (sichere) Aufbewahrung muss für jeden Standort individuell geprüft werden - aus baulichen Gründen - um sicherzustellen, dass Zugänge sowie Lifte in den Gebäuden vorhanden sind um die mobilen Notebookwagen zu transportieren oder die Notebookwagen werden in allgemeinen Räumen platziert. Zwecks Kalkulation wurde immer ein kompletter Notebookwagen berücksichtigt und Alternativen (mehrere kleinere Aufbewahrungssysteme) können in diesem Preisrahmen sein.
- Alle Preise sind aktuelle Marktpreise und Modellvarianten (der genannte Typ gilt nur als Referenz). Änderungen bei den Aufbewahrungsmodellen können aufgrund von neuen Schulraumaufteilungen vorkommen.
- In der Regel besteht die Mindestgarantie von 2 Jahren

2.5.4 Verwendung privater Geräte [BYOD]

Bei der Nutzung eines privaten Gerätes [BYOD] (Smartphone, Computer) durch Lehrpersonen oder anderen Mitarbeitenden der Schule, zur Verarbeitung schulischer Daten gilt grundsätzlich, dass es sich um ein sicheres und vor fremden Zugriffen geschütztes Gerät handeln muss. Folgende Aspekte sind in jedem Fall zu berücksichtigen:

- Aktuelles Betriebssystem
- Laufend aktualisiertes Antivirenprogramm
- Sicheres Passwort
- Kein Speichern von persönlichen Daten sowie Aufnahmen (Film, Foto) von Schülerinnen und Schülern oder Mitarbeitenden der Kreisschule Aarau-Buchs.

Aktualisierung: Neubeurteilung BYOD bei Lehrpersonen

Die Kreisschulpflege Aarau-Buchs hat anlässlich der Sitzung vom 30. März 2020 das Setting der persönlichen Geräte der Lehrpersonen gemäss 2.5.6 des Technischen Konzeptes ICT 2020+ gutgeheissen. Die Bedingungen müssen noch ausgearbeitet werden. Bei der Ausarbeitung der Bedingungen hat sich gezeigt, dass man die persönlichen Geräte der Lehrpersonen zwar auf das WLAN und die Schulsoftware zugreifen lassen kann, der Umstand dass diese jedoch ohne professionelle Wartung und Support benutzt werden, kann Schwierigkeiten mit der Kompatibilität und Nutzung der Peripherie (Drucker, Beamer etc.) mit sich bringen. Meist ist durch solche Geräte auch mit einem höheren Risiko an Sicherheitslücken zu rechnen bzw. deren Verhinderung bedeutet erhöhten Aufwand. Fällt ein Gerät während des Unterrichts aus, müssen die Lehrpersonen auf Geräte zurückgreifen, welche der Dienstleister der Schule bereitstellt, bei deren Anwendung sie an ihre Grenzen stossen könnten, aufgrund der abweichenden Bedienung. BYOD kann also umgesetzt werden, allerdings bringt es Risiken mit sich, welche als Schwächen der Gesamtumsetzung gedeutet werden können, auch wenn sie nur durch persönliche Geräte verursacht sind. Einer Neubeurteilung von BYOD bei Lehrpersonen, vor dem Hintergrund eines etablierten Betriebs und gesteigerter Anwendererfahrung, sollte zu einem späteren Zeitpunkt nichts im Weg stehen.

2.6 Formfaktor und Betriebssystem

Der Entscheid über den Formfaktor und dem Betriebssystem ist in Abhängigkeit der vorhergehenden pädagogischen Szenarien, basierend auf den Lehrplan 21:

- Tablet
- Convertible (2in1)
- Notebook
- Desktop

Gemäss der Softwareliste Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**, werden zukünftig grossmehrheitlich webbasierte Software eingesetzt.

Entscheidung:

- Für die SuS werden Tablets und Convertible (2in1) ausgewählt
- Für die LP werden Convertible (2in1) und Notebooks ausgewählt
- Vorerst keine Feststationen oder Desktops, denn die Ausnahmen: Bibliothek und Lehrervorbereitung wurden in diesem Konzept nicht berücksichtigt/kalkuliert!

In einem zukünftigen Pflichtenheft muss darauf geachtet werden, dass gerade bei den SuS und LP, die Windows Modelle vom gleichen Hersteller, respektive kompatibel in Bezug auf die Stromversorgung Netzteil und Dockingstation (unter den LP) sind.

2.6.1 Lebensdauer

Die Endgeräte-Lebensdauer hängt vom Einsatz und der Robustheit der Hardware stark ab. Kostengünstigere Geräte sind tendenziell vom eingesetzten Material (Gehäuse), Systemkomponenten, Akku und allgemein der Verarbeitung anfälliger als Geräte im normalen und höheren Preissegment. Die Garantie stellt nur die Systemmängel während der Laufzeit ohne äussere Einwirkung sicher, das heisst es gibt eine hohe Wahrscheinlichkeit für Ersatzteile beim Lieferanten/Hersteller. In den meisten Fällen ist bei einer Garantieverlängerung (nach der Kaufgarantie) der Akku ausgeschlossen! Teurere Geräte haben eine höherwertige Verarbeitung und sind so weniger anfällig auf äussere Schäden, die einen Ersatz/Reparatur benötigen.

Daraus schliesst sich folgende Übersicht:

Gerät / Komponente	Garantie	Preissegment [CHF]	Lebensdauer (Erfahrungswerte)	Hinweise
Preiswerte Consumer Convertible, Notebook, Tablet	12 Mt. / 24 Mt.	bis 600.--	2 bis 3 Jahre	Die Geräte werden mobil eingesetzt und werden dadurch stark beansprucht, so auch der eingebaute Akku. Ersatzteilbeschaffung und Reparatur sind eingeschränkt und der Austausch ist nicht immer möglich.
Small Business Convertible	24 Mt. / 36 Mt. / 60 Mt.	ab 900.--	4 bis 7 Jahre	Die Geräte werden mobil eingesetzt und werden dadurch stark beansprucht. Ersatzteilbeschaffung, Reparatur und Austausch sind eher möglich. Falls eine Garantieverlängerung vorhanden ist, kann der Lebenszyklus verlängert werden.
Business Convertible	24 Mt. / 36 Mt. / 60 Mt.	ab 1200.--	4 bis 7 Jahre	Die Geräte werden mobil eingesetzt und werden dadurch stark beansprucht. Ersatzteilbeschaffung, Reparatur und Austausch sind eher möglich. Falls eine Garantieverlängerung vorhanden ist, kann der Lebenszyklus verlängert werden.
Business Notebook	24 Mt. / 36 Mt. / 60 Mt.	ab 1200.--	4 bis 7 Jahre	Robuste Geräte vor allem für den stationären Einsatz. Mainboard Batterie, Netzteil, Lüfter oder Harddisks müssen eventuell vorher gewechselt werden.

Tabelle 8 Preissegment Windows Endgeräte

Hinweise:

- Ziel und Erwartung der Schule muss sein, ein Endgerät mit möglichst hoher Lebensdauer zu beschaffen, um Ausfälle und Ersatz während der Betriebsjahre grösstmöglich zu vermeiden. Somit kann ein wesentliches Investierungsrisiko vermieden werden.
- Bei einer Beschaffung soll eine Reserve zwischen 2–5% des Beschaffungsvolumens berücksichtigt werden, um bei Problemen (DOA, defekte Geräte, RMA) bei der Inbetriebnahme oder später im Betrieb schneller reagieren zu können. (Austausch für die Anwender)
- Möglichkeiten um die Endgeräte nach Ablauf der Lebensdauer an die Nutzer, gegen einen Betrag, (wiederaufbereitet) abzugeben kann berücksichtigt werden. Aufgrund der unterschiedlichen Nutzung und Einsätze der Endgeräte, können tendenziell die persönlichen 1:1 Endgeräte in Betracht gezogen werden.
- Die Lebens- oder Einsatzdauer wird mit 5 Jahren / 60 Monaten berechnet.

2.6.2 Ausstattung SuS

Für die SuS wird je ein Tablet und Convertible (2in1) vorgeschlagen:

- Modell Tablet (Apple iPad)
- Modell Convertible (Microsoft Windows)
- Für beide Modelle wird das entsprechende Zubehör aufgelistet

Tablet	Spezifikation
Apple iPad	Schulversion: Apple iPad 10.2" (2019), 128GB, Space Grey, WiFi, iOS 13 Wichtig: Inkl. DEP-Registrierung (Apple-Programm zur Geräteregistrierung)
Richtpreis	ca. CHF 450 inkl. MwSt. (Januar 2020)
Garantie	Auf ein (1) Jahr beschränkte Apple-Garantie - (SCHWEIZ)

Tabelle 9 Minimalanforderungen Tablet Spezifikation

Zubehör	Spezifikation
Schutzhülle	Universal und kompatibel zu den spezifizierten Endgeräten Tablets für SuS, beispielsweise Neopren Sleeve.
Richtpreis	ca. CHF 25.-- inkl. MwSt. (Januar 2020)
Garantie	Mind. 2 Jahre Herstellergarantie

Tabelle 10 Tablet Zubehör Schutzhülle

Convertible	Spezifikation
2in1	Education Konditionen [Beispiel: Microsoft Shape the Future-Program] Grösse mind. 12 Zoll Bildschirm (Auflösung mit Full HD) Mit Touchscreen, Wifi (aktueller Standard), CH-Tastatur (muss nicht abnehmbar sein), Gewicht max. 1.5kg, Prozessor: i5 (lüfterlos), Speicher SSD: mind. 128GB, Arbeitsspeicher: 8GB, Windows 10 Pro/Education Lizenz, Integrierte Kamera und Audio/Mikrofon, Bluetooth (BT), 3,5 mm Audiobuchse, Akkulaufzeit mind. 8h Zubehör: BT-Maus und ev. Stift (Pen) Hinweis: Externes Netzteil muss im Lieferumfang sein
Richtpreis	ca. CHF 900 - 1200 inkl. MwSt. (Januar 2020)
Garantie	Mind. 2 Jahre Herstellergarantie, erweiterbar und optional bis auf 5 Jahre

Tabelle 11 Minimalanforderungen Convertible Spezifikation SuS

Zubehör	Spezifikation
Notebooktasche	Universal und kompatibel zu den spezifizierten Endgeräten im 1:1 Setting für SuS
Richtpreis	ca. CHF 35.-- inkl. MwSt. (Januar 2020)
Garantie	Mind. 2 Jahre Herstellergarantie

Tabelle 12 Convertible Zubehör für SuS Notebooktasche

2.6.3 Ausstattung LP

Für die Lehrpersonen werden zwei Windows Modelle vorgeschlagen:

- Modell Convertible entspricht dem Modell für die SuS
- Modell Notebook entspricht den minimalen Spezifikationen des Convertible
- Inklusive notwendiges Zubehör

Convertible	Spezifikation
2in1	Education Konditionen [Beispiel: Microsoft Shape the Future-Programm] Grösse mind. 12 Zoll Bildschirm (Auflösung mit Full HD) Mit Touchscreen, Wifi (aktueller Standard), CH-Tastatur (muss nicht abnehmbar sein), Gewicht max. 1.5kg, Prozessor: i5 (lüfterlos), Speicher SSD: mind. 256GB, Arbeitsspeicher: 8GB, Windows 10 Pro/Education Lizenz, Integrierte Kamera und Audio/Mikrofon, Bluetooth (BT), 3,5 mm Audiobuchse, Akkulaufzeit mind. 8h Zubehör: BT-Maus und ev. Stift (Pen) Hinweis: Externes Netzteil muss im Lieferumfang sein
Richtpreis	ca. CHF 1200 - 1500 inkl. MwSt. (Januar 2020)
Garantie	Mind. 2 Jahre Herstellergarantie, erweiterbar und optional bis auf 5 Jahre

Tabelle 13 Minimalanforderungen Convertible Spezifikation LP

Notebook	Spezifikation
Notebook	Education Konditionen [Beispiel: Microsoft Shape the Future-Programm] Grösse mind. 14 Zoll Bildschirm (Auflösung mit Full HD) Optional Touchscreen, Wifi (aktueller Standard), CH-Tastatur, Gewicht max. 1.5kg, Prozessor: i5 (lüfterlos), Speicher SSD: mind. 256GB, Arbeitsspeicher: 8GB, Windows 10 Pro/Education Lizenz, Integrierte Kamera und Audio/Mikrofon, Bluetooth (BT), 3,5 mm Audiobuchse, Akkulaufzeit mind. 8h Zubehör: BT-Maus Hinweis: Externes Netzteil muss im Lieferumfang sein
Richtpreis	ca. CHF 1200 - 1500 inkl. MwSt. (Januar 2020)
Garantie	Mind. 2 Jahre Herstellergarantie, erweiterbar und optional bis auf 5 Jahre

Tabelle 14 Minimalanforderungen Notebook Spezifikation LP

Zubehör	Spezifikation
Dockingstation	Herstellerkompatible Dockingstation (am besten für beide Modelle Convertible & Notebook der LP) Inkl. Netzteil Anschluss: HDMI, USB, LAN,
Richtpreis	ca. CHF 150 - 200 inkl. MwSt. (Januar 2020)
Garantie	Mind. 2 Jahre Herstellergarantie, erweiterbar und optional bis auf 5 Jahre

Tabelle 15 Convertible und Notebook Zubehör für LP Dockingstation

Zubehör	Spezifikation
Notebooktasche	Universal und kompatibel zu den spezifizierten Endgeräten im 1:1 Setting für LP
Richtpreis	ca. CHF 35.- inkl. MwSt. (Januar 2020)
Garantie	Mind. 2 Jahre Herstellergarantie

Tabelle 16 Convertible und Notebook Zubehör für LP Notebooktasche

2.6.4 Erläuterungen

- Zwecks Vereinfachung in der Kalkulation wird der gemeinsame Richtpreis CHF 1200.-- des LP -Convertible und -Notebooks verwendet, so muss nicht detailliert erhoben werden, welcher Formfaktor durch die LP gewählt wird.
- Alle Richtpreise sind aktuelle Marktpreise ohne Sonderkonditionen für Grossmengen oder Spezialangebote, die in einer Ausschreibung erwartet werden können.
- Alle Endgeräte (ausser Apple) werden mit der Mindestgarantiedauer von 2 Jahren berechnet.
- Die Dockingstation muss kompatibel mit den beiden Convertible und -Notebooktypen sein.
- Bei den Windowsgeräten muss mindestens die Windows 10 Home Edition lizenziert sein. Ein Upgrade ist über das «Microsoft Shape the Future-Programm» möglich oder durch eine entsprechende Lizenzierung (Desktop EES) über den aktuellen educa-Rahmenvertrag.
- Im Preis der Windowsgeräte wurde ein Pre-Setting ab Werk berücksichtigt und wird zwingend empfohlen. Dieses kann ein Labeling (Beschriftung) beinhalten, das Setzen des Firmware-Schutzes (mittels Passwortschutz oder Zertifikat), Ausstellen der Geräte-ID und Seriennummer in Listenform und die Definition des Auslieferungszustandes und Version des Betriebssystems für eine reibungslose Integration.

2.7 Rahmenbedingungen

Die Konzeption stützt sich auf bewehrte und etablierte Services im schweizerischen Bildungsbereich verschiedener namhafter Hersteller. Daraus folgt eine Fokussierung auf die beiden Lösungsanbieter Microsoft und Apple. Die Infrastruktur wird im Microsoft Cloud Ecosystem abgebildet:

- Betriebssystem der Endgeräte: Microsoft Windows 10 oder Apple iOS
- Microsoft Office 365: Word, Excel, PowerPoint, Outlook, Teams
- Betriebssystemkompatible (Desktop-) Apps -> Schul- und Fachapplikationen
- Schulsoftware: Vorwiegend Web-/Browserbasierte Lösungen

Hinweis: Neben proprietärer Software können Open Source Lehrmittel geprüft werden, insofern diese den Kompatibilitätsanforderungen genügen.

Die nachfolgenden Rahmenbedingen werden sich im Lösungsansatz konkretisieren.

2.7.1 Professionelle Infrastruktur in den Schulen

Die technische Entwicklung mit Mischformen von 1:1/1:n Endgeräten, der Basisinfrastruktur der Schule und die Verlagerungen ins Netz verlangen nach verstärkter Koordination und Standardisierung. Zudem werden Schul- und Fachanwendungen oder Software nicht mehr eingekauft, sondern nutzungsbasiert lizenziert. Apps auf Tablets werden und müssen heute über die ganze Schule in einem MDM (Mobile Device Management) administriert und aufgesetzt werden. MDM ist ein Begriff aus der modernen IT-Arbeitsplatzverwaltung und steht für die zentralisierte Verwaltung von Mobilgeräten wie Tablets, Convertibles (2in1), Notebooks (Desktops) durch einen oder mehrere Administratoren mit Hilfe von Software und Hardware. Die Schulen sind durch diese Entwicklungen stark gefordert, den pädagogischen und den technischen Support weiterzuentwickeln. Grosse Schulen müssen dazu ihre technischen Dienstleistungen zentralisieren, um die verschiedenen Ebenen effizient und funktionsfähig zu verbinden.

Der Umgang mit mobilen Lösungen bedeutet, einfache Zugänge für Lehrpersonen sowie Schülerinnen und Schüler zu schaffen und ein schnelles und unkompliziertes Angebot zu ermöglichen. Somit ist eine Professionalisierung im Bereich Medien & Informatik an den Schulen unabdingbar, damit die Technik dem Lehren und Lernen dienen kann.

2.7.2 Umgang mit Apps, Software und Fachanwendungen

Software und Fachanwendungen werden durch den technischen Support angeschafft und lizenziert. Lehrpersonen melden den PICTS den Bedarf, diese klären und prüfen die Software und melden die Anschaffung an den technischen Support.

Apps auf Tablets werden via Mobile Device Management (MDM) angeschafft, lizenziert und organisiert. Mit einem MDM kann über die ganze Schule exakt bestimmt werden, welche Apps auf welchem Tablet installiert sein sollen. Lehrpersonen melden den PICTS den Bedarf, diese klären und prüfen das App und melden die Anschaffung dem technischen Support.

Auf einem SharePoint oder in einem Team des Office 365 werden die Anschaffungen und Lizenzierungen transparent gemacht mit konkreten Unterrichtsbeispielen, so dass für Lehrpersonen eine Sammlung von Anwendungsbeispielen zur Verfügung steht.

2.7.3 Netzwerk

***Ergänzung:** Das Netzwerkkonzept ist nicht Teil dieses technischen Konzeptes, sondern eines separaten Auftrages, welcher aktuell durch die IZAB umgesetzt wird.*

Ein separates Durch die künftige Fokussierung der Ausstattung auf mobile Endgeräte (Tablets, Convertibles, Notebooks), braucht es an jedem Standort zwingend ein sehr leistungsstarkes Internet/Netzwerk (Abonnement und interne Netzwerk Infrastruktur). Das aktuelle Abonnement Schulen ans Internet (SAI) von Swisscom (30/10Mbits/s) genügt diesen Anforderungen nicht mehr oder nur bedingt an kleineren Standorten, wie zum Beispiel der Kindergarten auf Platz Aarau. Künftig sind sogenannte «Business-Lines» sowie zeitgemässe Access-Points (AP) für flächendeckendes und leistungsstarkes WLAN notwendig. Bezüglich WLAN-Abdeckung wird eine vorgängige Ausmessung der WLAN-Hotspots empfohlen.

- Empfehlung Bandbreite pro Schulstandort (Up-/Download): 500/500Mbit/s synchron, wobei mindestens 200/200Mbit/s.
- Empfehlung WLAN Access-Points – Pro Schulzimmer ein AP (2.4/5.0 GHz) ac-Standard (1.3 Gbit/s und abwärtskompatibel zu älteren WLAN Standards.)

2.7.4 Datenschutz bei Cloud-Diensten

Aktuell werden im schweizerischen Bildungsbereich nur die Cloud-Dienste von Microsoft als Datenschutzkonform verifiziert. Darunter fallen grundlegende Dienste, die der Schule die Möglichkeit geben Datenablagen, Benutzerauthentifizierungen, E-Mail-Postfächer und weitere Dienste ergänzend oder komplett in die Cloud auszulagern.

Microsoft Schweiz mit den Office 365 Education Cloud-Diensten ist gegenüber Anbietern wie Apple oder Google (iCloud, Dropbox oder Google Drive) der einzige Anbieter der eine Vereinbarung und Ratifizierung mit educa.ch und privatim verabschiedet hat.

Die Apple und Google -Dienste können gemäss den Nutzungsrechten ähnliche rechtliche Konditionen anbieten, wobei diese nicht privatim oder educa-konform sind. Letztendlich ist immer der Nutzer von Cloud-Diensten in der Verantwortung gegenüber dem Service-Erbringer über den Inhalt der Daten, die er wissentlich in die Cloud stellt.

educa.ch nimmt seit 2017 als Fachagentur des Bundes und der Kantone Aufgaben bei der Qualitätsentwicklung im Bereich von Informations- und Kommunikationstechnologien (ICT) in der obligatorischen Schule und der Sekundarstufe II der Schweiz wahr.

privatim, die Konferenz der schweizerischen Datenschutzbeauftragten, will den Anliegen des Datenschutzes Nachdruck verschaffen. Sie fördert die Zusammenarbeit unter den Schweizer Kantonen, den Gemeinden und dem Bund auf dem Gebiet des Datenschutzes durch ständigen Informationsaustausch und ermöglicht so den wirkungsvollen Einsatz der Ressourcen.

Im Zusammenhang mit der Verwendung von Cloud-Diensten und Personendaten gelten für Schulen, die folgenden Gesetze auf Ebene Bund und Kanton:

- Bundesgesetz über den Datenschutz (DSG) von 1992 (in Revision)
 - Datenbearbeitung durch Dritte (Art. 10a; Art. 8 Rev.)
 - Grenzüberschreitende Datenbekanntgabe (Art. 6; Art. 13 Rev.)
 - Verletzung der beruflichen Schweigepflicht (Art. 35; Art. 56 Rev.)
- Verordnung zum Bundesgesetz über den Datenschutz (VDSG) von 1993
- Kantonale Datenschutzgesetzgebung
- Kantonale Gesetzgebung betreffend Informatik und Informationssicherheit

Personendaten - Art. 3 a DSG

«Alle Angaben, welche sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen.»

Besonders schützenswerte Personendaten - Art. 3 c DSG

«Personendaten, über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, über die Gesundheit, die Intimsphäre und die Rassenzugehörigkeit, über Massnahmen der sozialen Hilfe sowie über administrative oder strafrechtliche Verfolgungen und Sanktionen.»

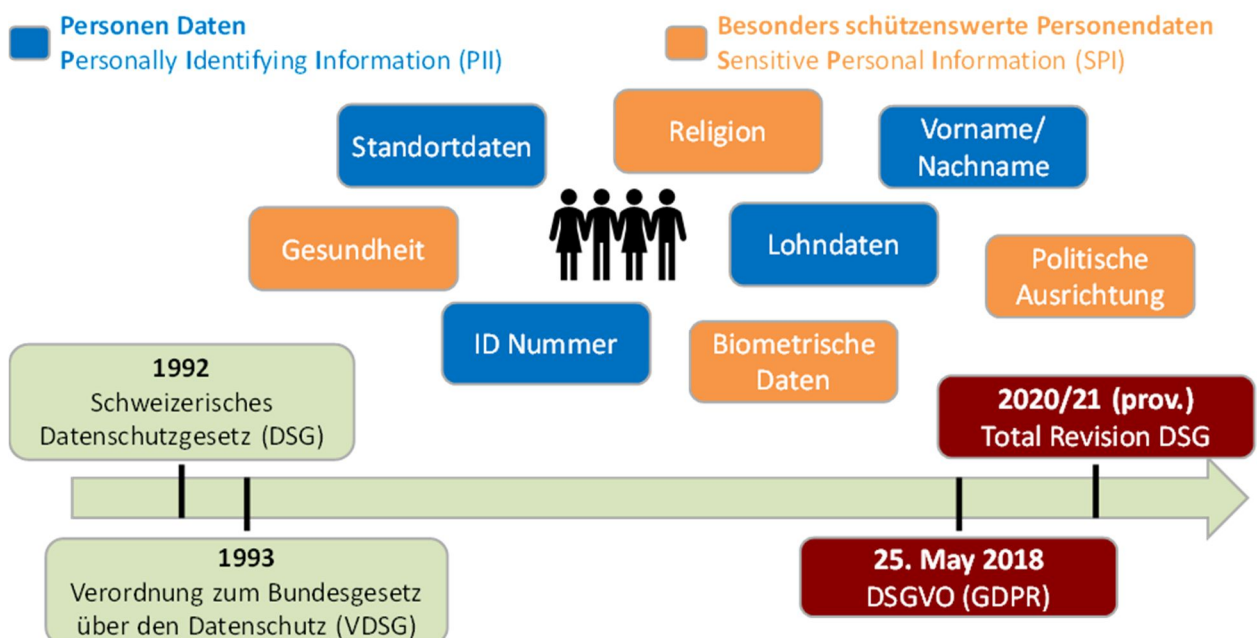


Abbildung 1 Personendaten und Datenschutz (DSG)

Wichtig:

Bei der Verwendung von Personendaten in der Cloud sind diese zu verschlüsseln, sowohl beim Transport (data in transit) als auch bei der Speicherung (data at rest). Bei besonders schützenswerten Personendaten sind zusätzliche Anforderungen an das Key-Management der jeweiligen Verschlüsselung zu stellen:

- Grundsätzlich dürfen die relevanten «Master-Keys» nur für die Schule verfügbar sein.

- Ist dies nicht möglich, können die «Master-Keys» beim Cloud-Anbieter aufbewahrt werden, wenn er sich vertraglich verpflichtet, sie nur mit der ausdrücklichen Zustimmung der jeweiligen Schule zu verwenden, und diese vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnissnahme geschützt sind. Die Zugriffe sind zu protokollieren.

2.7.5 Cloud & Plattformen

Microsoft & Office 365 Education

Microsoft Schweiz hat für die schweizerische Bildungslandschaft attraktive Angebote aus lizentechnischer Sicht. Seit mehr als 5 Jahren gibt es angepasste Office 365 Nutzungsbedingungen für Schweizer Bildungsinstitutionen, als Zusatzvereinbarung zum educa.ch Rahmenvertrag.

Microsoft Schweiz und educa.ch haben 2017 erneut einen weiteren, neuen Rahmenvertrag unterzeichnet, worin die Konditionen für die Nutzung von Desktop Plattformen, Office Produkte usw. definiert werden. Weiter wird die datenschutzrechtliche Situation beim Einsatz von Office 365 Cloud-Diensten für Schweizer Schulen geregelt. Der Rahmenvertrag entspricht den von der Vereinigung der kantonalen Datenschützer «privatim» definierten Rahmenbedingungen für den Einsatz von Cloud-Computing im Schulbereich.

Damit die angepassten Datenschutzbestimmungen für Office 365 zur Anwendung kommen, müssen Schulen Office 365 über einen Beitritt - unter dem educa.ch Rahmenvertrag - die Basisprodukte lizenzieren.

Das Microsoft Angebot für Bildungseinrichtungen ist kostenpflichtig. Hierzu sind Basislizenzen über einen Volumenlizenzvertrag jährlich zu beziehen. Wird ein Vertrag abgeschlossen können die Lehrpersonen und Schülerinnen und Schüler das Office Produkt auch privat kostenlos nutzen.

Der aktuelle **Rahmenvertrag** läuft im Juli 2020 aus. Es wird davon ausgegangen, dass es eine Verlängerung oder Erneuerung des Vertrages geben wird. In den aktuellen Verhandlungen werden die neuen Konditionen im Sinne der schweizerischen Bildungslandschaft ausgehandelt.

Datenhaltung in Schweizer Datencenter. Microsoft Schweiz wird die Office 365 Clouddaten für Education mittelfristig bis spätestens im Jahre 2022 in der Schweiz speichern. Weitere Informationen: https://www.innovativeschools.ch/IT_Schulgeraete/IT_Verwaltung/2839_Office_365_im_Schweizer_Datencenter.htm und **Fehler! Verweisquelle konnte nicht gefunden werden..**

2.7.6 Umsetzung ICT-Konzept 2020+

Die Kreisschule Aarau-Buchs hat zum Ziel, spätestens auf das Schuljahr 2022/2023 mit der Einführung der neuen Konzeption zu beginnen. Die Herausforderung, bezüglich gestaffelter oder vorzeitiger Einführung besteht weiterhin. Ein Ziel kann sein, aufgrund dieser Konzeption teile der Schule vorgängig auszurüsten, anstelle einer «grossen und einmaligen» Beschaffung über einen Betriebszeitraum von mindestens 5 Jahren.

2.8 IST-Analyse

Es können die nachfolgenden Endgeräte sowie Peripherie, die entsprechend kompatibel sind, im zukünftigen System eingebunden werden. Zu berücksichtigen ist, dass bestehende Endgeräte fortwährend auf einen aktuellen Stand gehalten werden müssen, in Bezug auf Betriebssystemversion und Sicherheitsupdates.

2.8.1 Endgeräte

Die Grundlagen sind in verschiedenen Inventarlisten aufgeführt, unter anderem mit dem Datum der Inbetriebnahme oder Beschaffungszeitpunkt. Nachfolgende Feststellungen:

<p>Inventarliste Aarau: 01_Inventar_Aarau.pdf</p> <ul style="list-style-type: none"> ➔ Die letzten/jüngsten Notebooks wurden im Jahre 2015 in Betrieb genommen -> 12 MacBook und 29 iMac. Bei einer Einsatzdauer von 6 Jahren sollten diese «neueren» Geräte wiederum ersetzt werden -> Fazit: 0% Weiterverwendung
<p>Inventarliste Hardware Kreisschule Buchs Rohr: 02_Inventarliste_KSBR.xlsx</p> <ul style="list-style-type: none"> ➔ Die letzten/jüngsten Desktop/Notebooks/Tablets wurden gem. Inventarliste im Juni 2017 beschafft. ➔ Die jüngsten Desktop-Computer wurden im Jahr 2017 beschafft für den Informatikraum in Rohr -> Fazit: 0% Weiterverwendung ➔ 102 iPads aus dem Jahre 2017 (verwaltet über einen Mac Mini mit Serversoftware zur Verwaltung der iPads) -> Diese können bis 2022 weiterhin verwendet werden, insofern die iOS-Version mit den angewendeten Apps kompatibel ist. ➔ Im Jahre 2019 wurden ca. 30 neue «Windows 10» Notebooks beschafft Fazit: 100% Weiterverwendung in Abhängigkeit der Betriebssystemversion.
<p>Export KSAB: 03_Arbeitsplatz_Inventar_KSAB.xlsx</p> <ul style="list-style-type: none"> ➔ Keine Angaben zur Beurteilung. Aufgrund der Beschreibung werden in dieser Liste ausschliesslich Arbeitsgeräte der Verwaltungsmitarbeitenden aufgelistet. ➔ Diese Arbeitsplätze sind nicht betroffen, da diese von der IT der Stadt betreut werden.
<p>Budgetierte und geplante Beschaffungen im Jahre 2020 an der KSAB:</p> <ul style="list-style-type: none"> ➔ An der Bezirksschule Aarau werden 30 LP-Endgeräte (Notebooks) beschafft. ➔ In Buchs werden 60 Convertibles (Lenovo) beschafft. ➔ Im OSA werden 24 iPads beschafft.

Tabelle 17 Inventarlisten

Zusammenfassend:

	Beschaffungsjahr	Lebensende	Erneuerung/Bemerkung
Ausgangslage -neue Geräte			
Beschaffungen im Jahre 2022	2022	2027	Nach 5 Jahren; Geräte Erneuerung ab Schuljahr 2027/28
Bestehende Geräte			
102 iPads	2017	2022	Nach 5 Jahren; Geräte Erneuerung ab Schuljahr 2022/23 -> in diesem Beschaffungsprojekt
30 neue W10-Notebooks	2019	2024	Ersetzen ab 2024
30 LP-Endgeräte (Notebooks)	2020	2025	Ersetzen ab 2025
60 neue W10-Convertibles	2020	2025	Ersetzen ab 2025
24 iPads	2020	2025	Ersetzen ab 2025

Tabelle 18 Lebenszyklen der bestehenden Endgeräte

Bemerkungen:

- Die 102 iPads müssen mit dem neuen Projekt ersetzt werden
- Die weiteren Endgeräte werden in der Berechnung in den Jahren 2024 oder 2025 ersetzt, während der neuen laufenden 5-jährigen Betriebsphase.

Hinweise:

- Bei der Wiederverwendung von bestehenden Endgeräten in ein neues Informatiksystem, müssen diese entsprechend vor- und aufbereitet werden. In der Regel werden diese Endgeräte auf Werkseinstellung (Wiederherstellung) zurückgesetzt, aktualisiert und in das neue Schulinformatiksystem eingebunden, insofern die technischen Voraussetzungen der Endgeräte gegeben sind.
- Für eine Übergangs- oder zukünftige Nutzung in der Beurteilung der Endgeräte müssen mindestens folgende Angaben vorliegen:
 - Die Betriebssystem Version der Endgeräte: iOS Version & Build / Microsoft Windows Version & Build
 - Den Beschaffungszeitpunkt und die Garantiedauer
 - Bemerkung zur Garantiedauer: Alle Apple Produkte wurden mit einer minimalen Garantiezeit von einem Jahr beschafft.
 - Der Formfaktor: Tablet, Convertible (2in1), Notebook, Desktop

2.8.2 Peripherie

***Ergänzung:** Peripheriegeräte, insbesondere Interaktive Wandtafeln (IWT) und Drucker sind nicht Teil dieses Konzeptes. Sie werden zusätzlich in den Dienstleistungsauftrag der IZAB integriert. Die daraus resultierenden Kosten werden aktuell durch die IZAB berechnet.*

Aktuell sind verschiedene interaktive Wandtafel und Druckerkonzepte im Einsatz. Bezüglich der zukünftigen Ausrichtung muss sichergestellt werden, dass die entsprechenden Endgeräte mit den interaktiven Wandtafeln (Smart Board), Beamer, Dokucam und den entsprechenden Druckerkonzepten verbunden werden können.

Es müssen die physischen und virtuellen Schnittstellen bekannt geben werden, wie beispielsweise:

- Verbindung übers Netzwerk LAN/WLAN
- Audio/Video Ausgänge
- WiFi/Bluetooth -Lösungen
- Druckeroptionen Netzwerk, Printserver, usw.

2.8.3 Netzwerk

Der Netzwerkteil ist «out-of-scope» in der Analyse und wird in einem separaten Projekt beleuchtet. Dieses Konzept kann bezüglich Netzwerks (Connectivity & Security) lediglich Empfehlungen abgeben.

***Ergänzung:** Aktueller Stand siehe 2.7.3*

3. Lösungsansatz

Die nachfolgend skizzierte Lösung basiert auf einem Cloud-only Ansatz. Das heisst es wird auf eine vor Ort Server Infrastruktur komplett verzichtet. Als Cloud Dienstleister wird Microsoft mit den Office 365 Services empfohlen.

Für den Cloud-only Ansatz sprechen die folgenden Punkte:

- ✓ Die Daten stehen ohne zusätzliche Infrastruktur sowohl von intern als auch extern zur Verfügung
- ✓ Kein eigene Server Infrastruktur, welche betrieben, verwaltet und periodisch ersetzt werden muss
- ✓ Der Betrieb der eigentlichen Infrastruktur wird vom Anbieter, sprich Microsoft sichergestellt
- ✓ Der Anbieter verfügt jeweils über alle notwendigen Zertifizierungen im Bereich Datensicherheit und Datenschutz (Z.B. ISO 27001 - internationale Standard für Informationssicherheit)
- ✓ Die Sicherheit und Verfügbarkeit der Services, wie etwa E-Mail oder Teams, liegt in der Verantwortung von Microsoft und ist vertraglich geregelt
- ✓ Die «echte» Nutzung von Kollaborations-Werkzeugen, wie etwa Microsoft Teams für die zentrale Ablage von Informationen und das gemeinsame Arbeiten an Dokumenten unabhängig von Zeit und Ort
- ✓ Skalierbarkeit – Zusätzliche Benutzer und/oder Speicherplatz können jederzeit auf Knopfdruck ergänzt werden
- ✓ Elastizität – Temporäre Erweiterung sind jederzeit möglich, um eventuelle Spitzen zu brechen, diese können danach auch wieder entfernt werden → Kostenoptimierung
- ✓ Sichere Integration von privaten Smartphones und Tablets
- ✓ Die Daten stehen auf den Devices sowohl online als auch offline zur Verfügung. Die offline bearbeiteten Daten werden automatisch nach Office 365 synchronisiert sobald wieder eine Internetverbindung hergestellt worden ist
- ✓ Die Schule kann sich auf die relevanten Themen pädagogischen Integration und Digitalisierung konzentrieren
- ✓ Die Lösung ist flexibel und unterstützt sowohl ein 1:1 Konzept bei der die Schule sämtliche Devices beschafft als auch BYOD Ansätze in den unterschiedlichsten Ausprägungen

Bei einem Cloud-only Ansatz müssen den folgenden Punkten besonders Beachtung geschenkt werden:

- Eine stabile, verfügbare und performante Internetverbindung an allen Schulstandorten ist eine Grundvoraussetzung für einen einwandfreien Betrieb
- Ein flächendeckende und moderne WLAN-Infrastruktur an allen Standort ist eine zwingende Anforderung
- Die Daten liegen an einem «fremden» Ort, das heisst eine Datensicherung zu einem Dritt-Anbieter wird empfohlen
- Der Umgang mit besonders schützenswerten Personendaten, welche sich in unstrukturierten Dokumenten wie etwa einer Worddatei befinden muss geregelt werden

3.1 Architektur

Die folgende Darstellung zeigt den schematischen Aufbau:

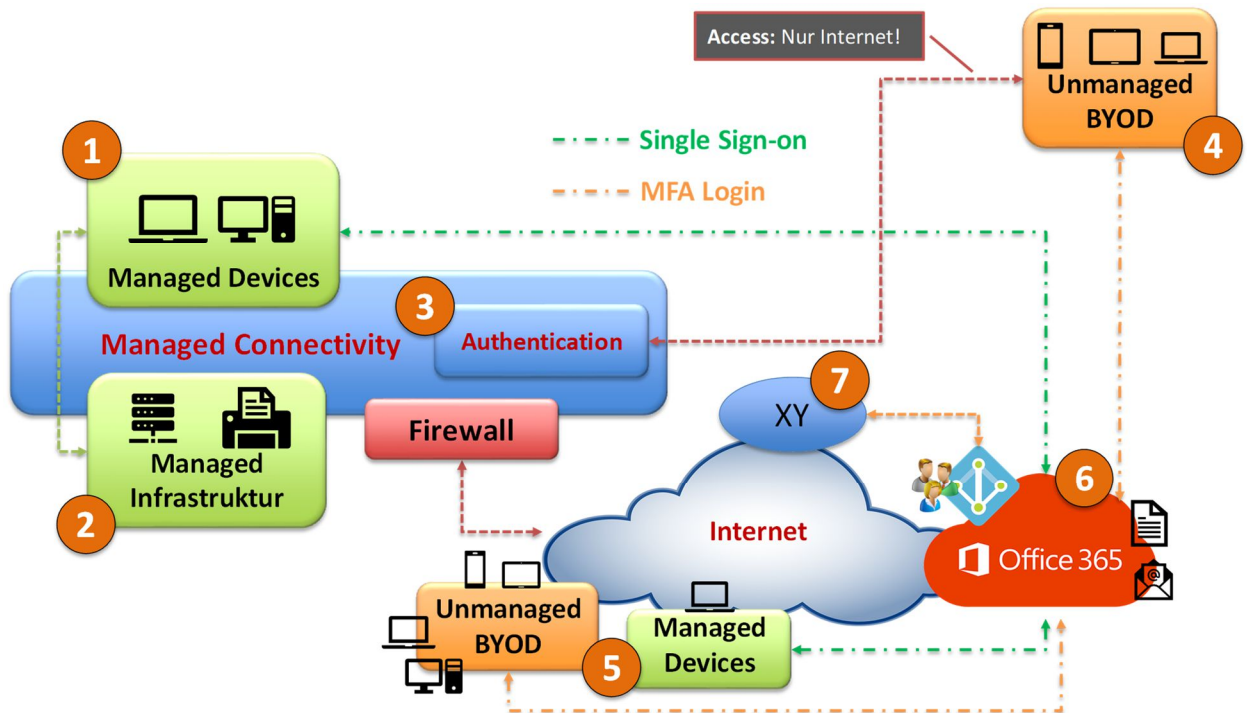


Abbildung 2 Schematischer Aufbau

- 1) **Managed Devices:** Von der Schule beschaffte und verwaltete Devices. Z.B.: Computer in dedizierten Informatikräumen oder Notebooks.
- 2) **Managed Infrastruktur:** Schuleigene Infrastruktur, wie etwa Drucker oder ein lokales NAS (Network Access Storage).
- 3) **Managed Connectivity:** Von der Schule beschaffte und verwaltete Netzwerk Komponenten (LAN, WLAN und Firewalls)
 - a. **Managed Device:** Die Verbindung benötigt keine zusätzliche Authentisierung → Empfehlung: Device Zertifikat
 - b. **Unmanaged Device:** Die Verbindung benötigt eine zusätzliche Authentisierung → Empfehlung: Captive Portal & SMS
- 4) **Unmanaged BYOD:** Mobile und nicht verwaltete, private Devices, welche im oder unterstützend für den Unterricht verwendet werden. Z.B.: private Smartphones oder Tablets

Datenzugriff und Konnektivität:

 - a. **iOS / Android:** Zugriff auf Office 365 Daten nur von verwalteten Apps möglich (z.B.: Word, Teams oder Outlook)
 - b. **Unbekanntes Betriebssystem:** Zugriff auf Office 365 Daten nur mittels Browser möglich und ohne Datei Up- oder Download. Bei der Anmeldung in Office 365 wird neben Benutzernamen und Passwort ein zweiter Faktor (Z.B. SMS) benötigt.
 - c. **Konnektivität:** Ein BYOD hat nur Zugriff auf das Internet und gegebenenfalls auf einzelne Drucker. Der Internetzugriff wird mit zusätzlichen Services gegen Schadsoftware geschützt und verfügt über einen Content-Filter für das Blockieren von unerwünschten Inhalten.
- 5) Befindet sich ein Device ausserhalb des von der Schule verwalteten Netzwerks (Z.B. zu Hause) so kann mit beiden Device Typen in der gewohnten Art gearbeitet werden.

Ausnahme: Die Schuleigene Infrastruktur (managed Infrastruktur) steht nicht zur Verfügung.

- 6) Alle benötigten Services wie etwa E-Mail, Datenablage oder ähnliches werden durch Office 365 zur Verfügung gestellt.
- 7) Weitere Services aus der Cloud von Drittanbietern sollten, wenn immer möglich eine Schnittstelle oder Federation in das Azure AD anbieten. Damit wird sichergestellt, dass sich der Benutzer nicht mehrere Anmeldeinformationen merken muss → Single Sign-On

Hinweis: Wird weiterhin eine On-Premises, sprich lokale Datenablage benötigt so muss dies entsprechend begründet werden. Die Bereitstellung kann über zwei Arten erfolgen.

- Ein lokales NAS, die Sicherung kann dabei von einem externen Backup Anbieter bereitgestellt werden. Der Zugriff, sprich die Authentisierung muss mit einem Azure AD Account möglich sein.
- Die Stadt stellt entsprechenden Speicherplatz inkl. Backup zur Verfügung. Der Zugriff, sprich die Authentisierung muss ebenfalls mit einem Azure AD Account möglich sein.

Es wird empfohlen immer zuerst zu prüfen, ob sich eine Anforderung nicht mit einem Cloud Service umsetzen lässt.

3.2 Infrastruktur-Services

3.2.1 Benutzer-Identität

Die Benutzer-Identität, sprich Benutzername und Passwort werden zentral im Microsoft Azure AD verwaltet. Es wird empfohlen die Benutzerstammdaten aus der bestehenden Schulverwaltungssoftware direkt in das Azure AD zu synchronisieren:

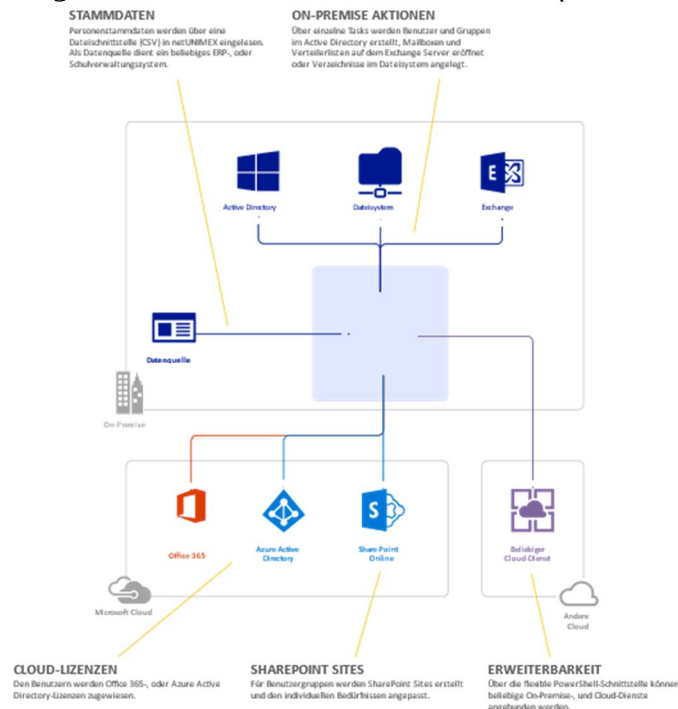


Abbildung 3 Schnittstelle SIS - Azure AD

Der Benutzer hat die Möglichkeit ein vergessenes Passwort eigenständig zurückzusetzen. Die Bestätigung der Identität erfolgt dabei mittels Smartphone. Der Benutzer ist Mitglied von definierten Sicherheitsgruppen und erhält damit Zugriff auf entsprechende Office 365 Ressourcen.

Hinweis: Für den Zugriff auf Office 365 Services von unbekanntem Devices wird bei der Anmeldung vom Benutzer ein zweiter Faktor verlangt. Dies kann eine SMS oder die Bestätigung in der Microsoft Authenticator App sein.

3.2.2 Printing

Das Drucken in grösseren Umgebungen ist heute eine echte Herausforderung und nicht mehr einfach mit der Bereitstellung von ein paar Druckern in Zimmern und Gängen erledigt. Vielmehr müssen Punkte wie etwa Datenschutz oder das Drucken von unterschiedlichen Endgeräten aus berücksichtigt werden.

Eine moderne Druckerlösung in einer Cloud-only Architektur sollte die folgenden Anforderungen erfüllen:

- **Datenschutz:** Ein Benutzer kann Druckaufträge einfach ins Netzwerk senden und diese erst ausdrucken, wenn er selbst vor Ort ist, um sie persönlich aus dem Drucker zu entnehmen. Bis zu diesem Moment kann er sich darauf verlassen, dass die Dokumente sicher aufgehoben sind.
- **Kostenkontrolle:** Mit der Zuweisung von Druckaufträgen zu den jeweiligen Benutzern wird eine effiziente Kostenkontrolle möglich. Im Weiteren sollen Regeln definiert werden können bezüglich monatlichem Druckvolumen oder ähnlichen Einschränkungen.
- **Webprinting:** gibt Nutzern die Möglichkeit, über ihre eigenen Mobilgeräte oder BYOD zu drucken, ohne erst einen Druckertreiber installieren zu müssen.
- **E-Mail Printing:** Dies ist die einfachste Lösung um von jedem Gerät (iOS, Android, Windows, Blackberry, Mac OSX, Linux) zu drucken, das E-Mail versenden kann.
- **Integration in das Azure AD:** Notwendige Benutzeranmeldungen sollen mit dem vorhandenen Azure AD Account durchgeführt werden.

Hinweis: Es wird empfohlen zu prüfen, ob die kompletten Drucker Infrastruktur nicht einfacher und effizienter als kompletter Service bezogen werden soll.

3.2.3 Microsoft Office 365

Microsoft Office 365 ist unter anderem eine Arbeits- und Kommunikationsplattform für Schulen. Das Office 365 ist eine Gesamtlösung mit E-Mail (Exchange Online), Office und App/Applikationen, Microsoft Teams (Kollaboration), SharePoint (gemeinsame Datenablage) sowie der Cloudspeicherlösung OneDrive for Business (persönlicher Datenspeicher).

An allen Schulstufen kann die interne Zusammenarbeit ausschliesslich über Office 365 erfolgen und die Funktionen des Office 365 können sehr breit angewendet und eingesetzt. Dies hat zur Folge, dass die Anwender einen Office 365 Account (mit oder ohne E-Mail-Adresse) bekommen und mit diesem Login, Zugang zu allen wichtigen Office Applikationen auf verschiedenen Endgeräten erhalten.

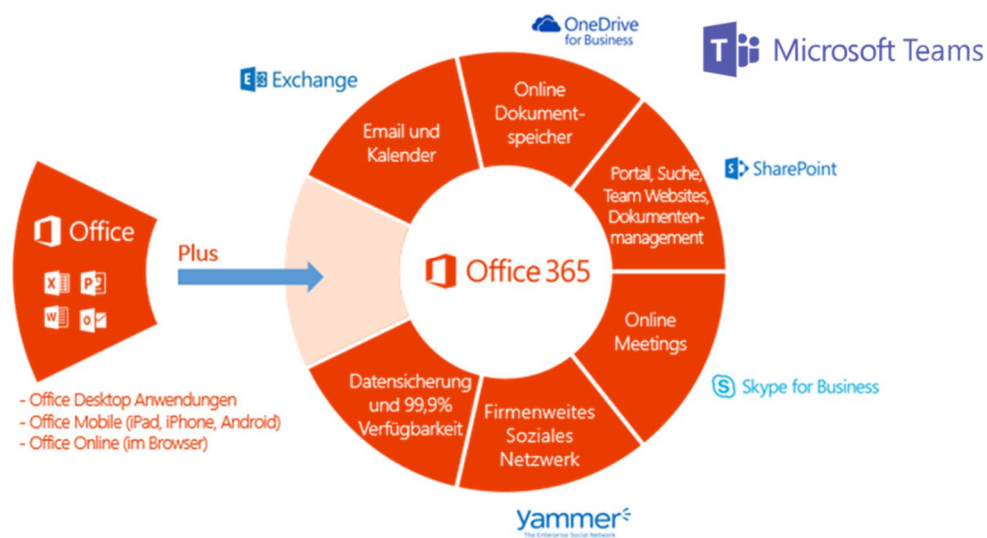


Abbildung 4 Office 365 Education

3.2.4 Microsoft Intune (MDM-Lösung)

Microsoft Enterprise Mobility + Security vereint eine Reihe von zusammenarbeitenden SaaS Lösungen (innerhalb von Microsoft Azure), um die modernen Endgeräte und Arbeitsweisen der Benutzer zu verwalten, steuern und zu schützen.

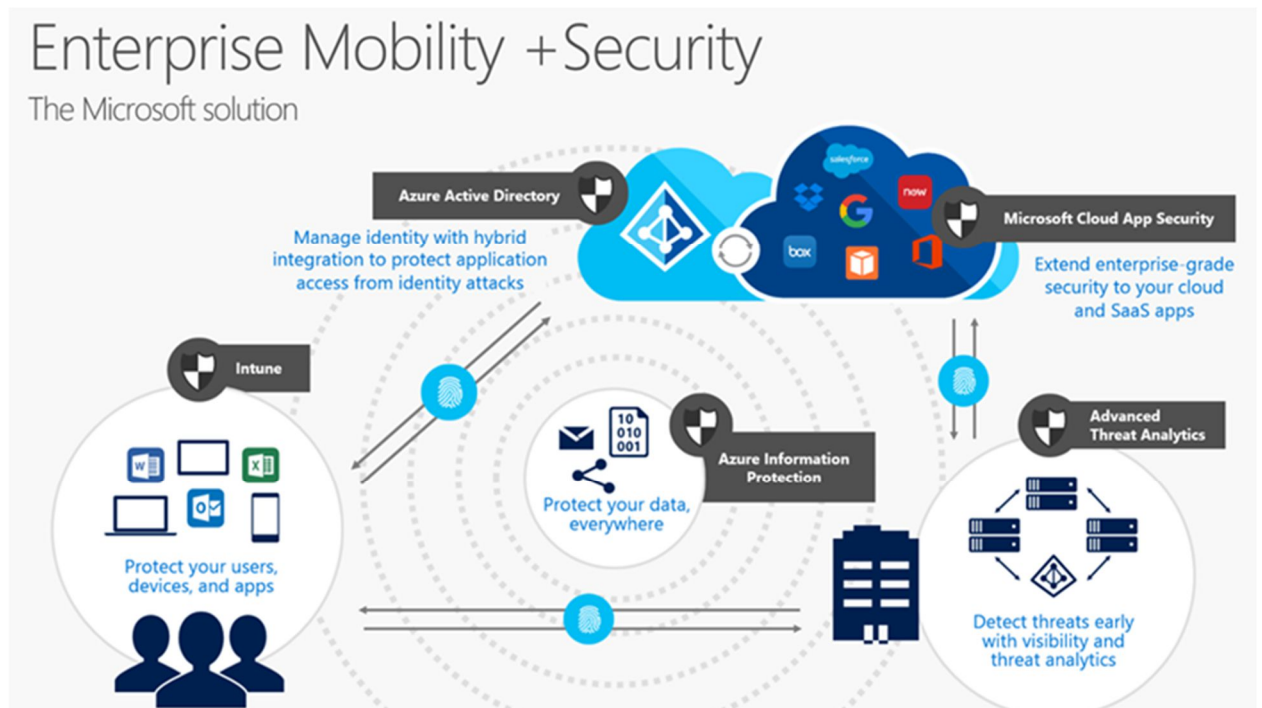


Abbildung 5 Übersicht MDM EM+S

Microsoft beschreibt Enterprise Mobility + Security als eine identitätsbasierte Sicherheitslösung, die einen ganzheitlichen Ansatz für die Sicherheitsherausforderungen in der heutigen Zeit von «Mobile First» und «Cloud First» bietet. Die Technologien helfen nicht nur die Verantwortlichen zu schützen, sondern Verstöße zu erkennen bevor diese zu Schäden führen. Die EM+S ist ein Paket von Produkten, die mit einem einzigen Abonnement pro Benutzer zusammengeführt und lizenziert werden, das folgende Produkte beinhaltet:

Identity and Access Management	Device and App Management	Information Protection + Security
-Azure Active Directory Premium -Multi-Factor Authentication -Microsoft Identity Manager	-Microsoft Intune -System Center Configuration Manager	-Azure Information Protection -Advanced Threat Analytics -Cloud App Security

Tabelle 19 Enterprise Mobility + Security Produkte

Fazit:

- Microsoft Intune aus der EM+S Suite wird als MDM-Lösung vorgeschlagen.
- Der **Microsoft Enterprise Mobility + Security A3** -Plan enthält folgende Features:
 - Azure Active Directory Premium P1
 - Microsoft Intune (for Education)
 - Azure Information Protection Premium P1
 - Microsoft Advanced Threat Analytics

3.2.5 Erweiterte Sicherheit (Advanced Security)

Im Zusammenhang mit einer erweiterten Verschlüsselung der Datenspeicherung in der Cloud, wurden als Option, weitere Sicherheitsfunktionen berücksichtigt und berechnet. Diese sind zwingend in einer ganzheitlichen Cloud-Infrastruktur-Lösung zu prüfen.

Mit dem **Office 365 E5 Add-On**, werden erweiterte Sicherheits-, Analyse- und Sprachfunktionen, sowie Exchange Online Advanced Threat Protection für sichere Postfächer zur Verfügung gestellt. Die enthaltenen Funktionen sind:

- Zuverlässige Sicherheit
 - Advanced Threat Protection schützt Benutzer vor versteckten Bedrohungen in E-Mails, Anlagen und Links.
 - Mit der **Kunden-Lockbox** kann der Administrator den Datenzugriff beschränken, indem er die zweistufige Authentifizierung voraussetzt.
- Erweiterter Informationsschutz
 - Verhinderung von Datenverlust und Verschlüsselung in Exchange Online, Microsoft Teams und SharePoint Online sorgen dafür, dass die Inhalte in E-Mails, Chats und Besprechungen sowie auf Teamwebsites gut geschützt sind.
- Threat Intelligence
 - Threat Intelligence liefert fundierte Einblicke in die Bedrohungslandschaft.
- Intelligente Compliance-Lösungen
 - Mit dem Security & Compliance Center werden Richtlinien mühelos eingehalten und schützen die Daten mit den in Office 365 enthaltenen Lösungen wie eDiscovery, Data Governance und Überwachung.
- Cloud Access Security Broker
 - Office 365 Cloud App Security: Analyse und Bekämpfung von Cyberbedrohungen.
- u.v.m.

Datenschutz und Compliance optimieren

Eine sichere Schlüsselverwaltung ist von essenzieller Bedeutung, um Daten in der Cloud zu schützen. Mit **Azure Key Vault** können Schlüssel und Geheimnisse, wie z.B. Kennwörter (Passwörter) verschlüsselt werden.

Fazit:

- **Office 365 E5 Add-On** wird als Option im Zusammenhang mit **Azure Key Vault** vorgeschlagen, um die erweiterten Sicherheitsbedürfnisse abzudecken. Denn die Cloud, wird zukünftig die zentrale Infrastruktur sein.

3.2.6 Datenschutz und Datenablage (File Ablage)

Die Ablage von unstrukturierten Daten (Word, Excel, PDF, etc.) erfolgt komplett in Office 365. Dort werden die Dateien in Microsoft Teams oder SharePoint Bibliotheken abgelegt.

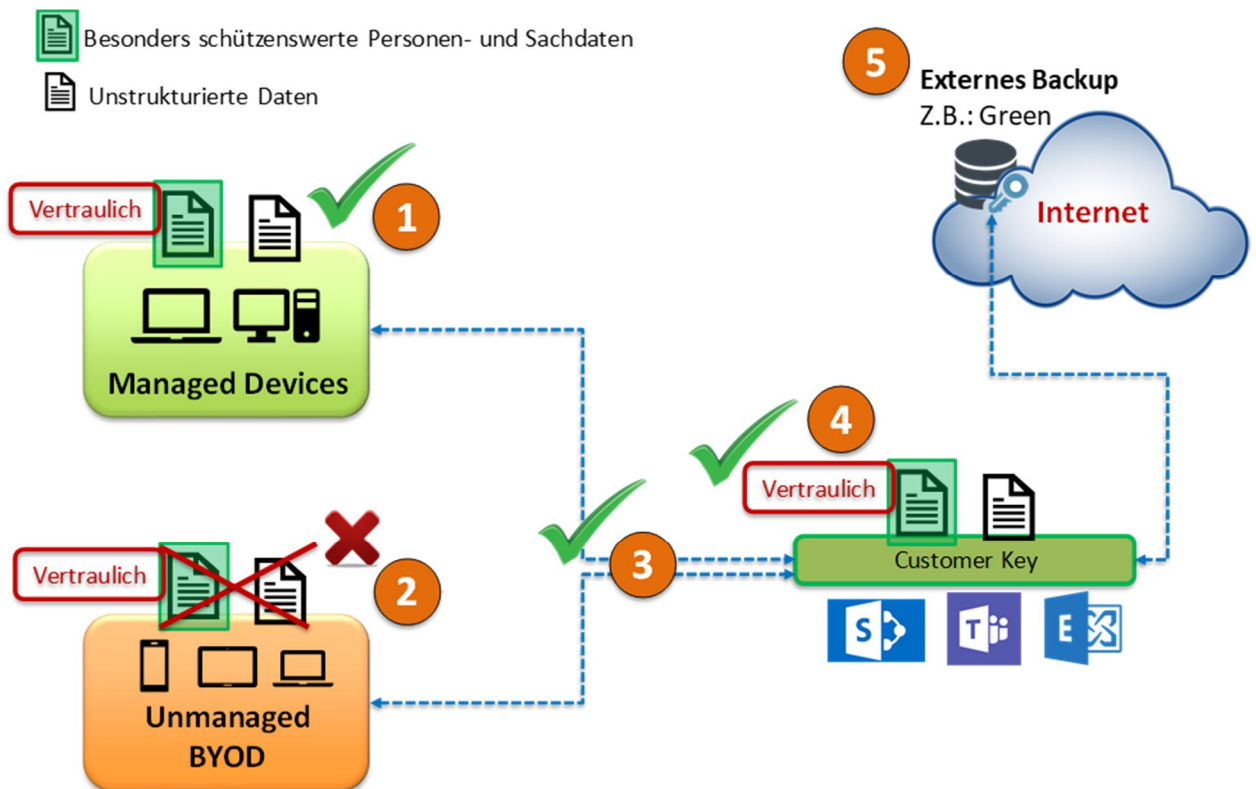


Abbildung 6 Datenschutz und Datenablage

Die Lösung berücksichtigt die Anforderungen der aktuellen Datenschutzbestimmungen und lässt sich für zukünftige Anforderungen (neues DSGVO) entsprechend erweitern.

- 1) Auf allen «managed» Devices ist die lokale Festplatte verschlüsselt und der dazugehörige Master-Key ist im Besitz der Schule.
- 2) Auf allen «unmanaged» Devices kann nicht davon ausgegangen werden, dass die lokale Festplatte verschlüsselt ist.
 - a. **iOS / Android:** Zugriff auf Office 365 Daten nur von verwalteten Apps möglich (z.B.: Word, Teams oder Outlook).
 - b. **Unbekanntes Betriebssystem:** Zugriff auf Office 365 Daten nur mittels Browser möglich und ohne Datei Up- oder Download. Bei der Anmeldung in Office 365 wird neben Benutzernamen und Passwort ein zweiter Faktor (z.B. SMS) benötigt.
- 3) Der Transport der Daten zwischen Device und dem jeweiligen Office 365 Service ist immer verschlüsselt (TLS).
- 4) Die Ablage der Daten in Office 365 in den Microsoft Rechenzentren ist immer verschlüsselt. Das heißt auf den physischen Datenträgern befinden sich ausschliesslich verschlüsselte Daten.
 - a. Standardmässig ist Microsoft im alleinigen Besitz des Master Key und die Schule hat keinen direkten Zugriff darauf.
 - b. Für die Einhaltung der Datenschutzbestimmungen in Bezug auf besonders schützenswerte Personendaten kann der optionale Service «Customer Key» lizenziert werden. Damit fällt das Management der Master-Keys in die Hände der Schule.

- 5) Es wird empfohlen die Datensicherung, sprich Backup aller von der Schule als relevanten Informationen klassifizierten Daten zu einem Dritt-Anbieter auszulagern. Damit kann die Unabhängigkeit zu Microsoft gewährleistet werden.

3.2.7 Managed Device

Alle von der Schule verwalteten Devices (W10 und iOS) werden mit dem Microsoft Online Service Intune bereitgestellt und verwaltet. Damit wird auch die Inventarisierung (HW und SW) aller Devices sichergestellt.

Im Folgenden wird die automatisierte Bereitstellung eines Windows 10 Devices beschrieben:

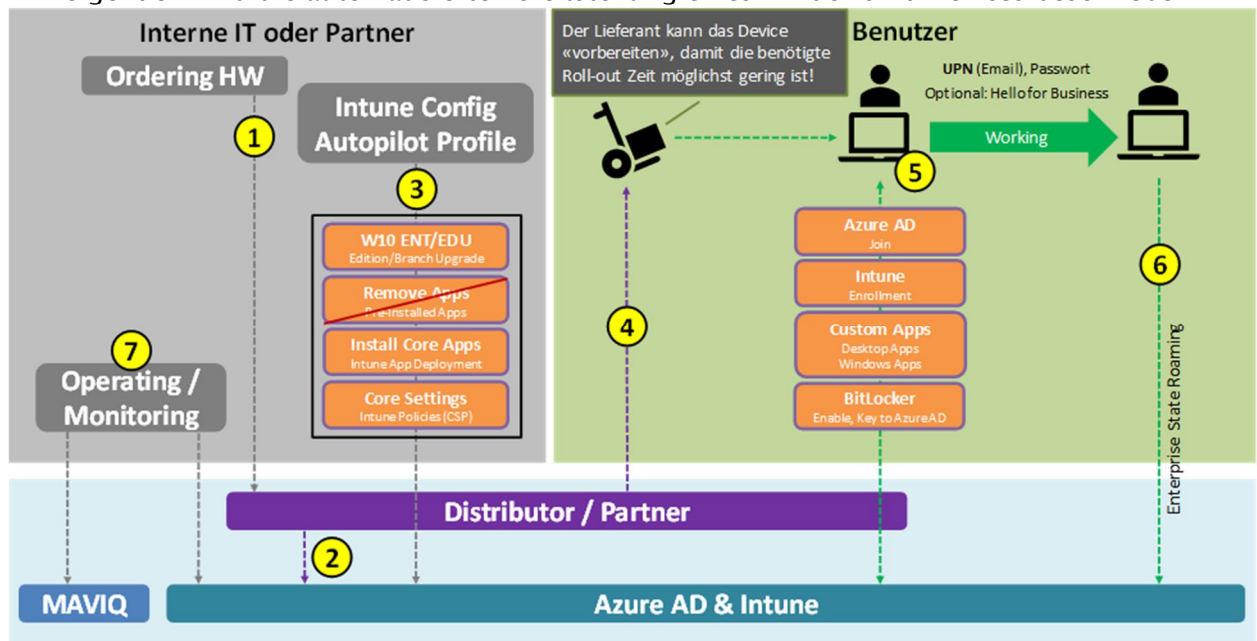


Abbildung 7 Bereitstellungsprozess Endgerät

- 1) **Bestellung** der Hardware:
 - a. BIOS Settings werden durch den Kunden festgelegt
 - b. Autopilot Registrierung durch den Lieferanten / Hersteller / Partner
 - c. Der Hersteller liefert eine Clean-OS Installation ohne Bloatware
- 2) **Autopilot:** Registrierung durch den Lieferanten im Kunden Office 365 Tenant
 - a. Device ID
 - b. Serial-Nr.
- 3) **Intune:** Richtlinien und Applikationen bereitstellen und zuweisen
 - a. **Autopilot:** Profil erstellen und zuweisen
 - b. Standard-Richtlinien gemäss Detailkonzept
 - c. Security-Richtlinien gemäss Detailkonzept
 - d. Applikationen (W32 und Windows Apps) gemäss Liste
- 4) **Lieferung** der Devices direkt an den benötigten Standort
 - a. Optional können die Devices für ein «Pre-Staging» zu einem Partner geliefert werden. Damit wird der Benutzer Roll-out Prozess (#5) deutlich beschleunigt
- 5) **Inbetriebnahme bzw. Roll-out** des Devices durch den Benutzer → der Autopilot Wizard erscheint und der Benutzer muss sich mit seinen Logindaten anmelden (Benutzername und Passwort)

- a. **Intune** Automatisches Setzen der Konfigurationen und Installation der zugewiesenen Applikationen
- 6) **Azure AD:** Das Gerät wird dem Benutzer zugewiesen und die Benutzerprofil Daten werden in der Azure gespeichert → Enterprise State Roaming
- 7) **Betrieb, Monitoring** (inkl. Windows Defender Monitoring & Notification) und **Inventarisierung**

Hinweis: Der Benutzer kann selbständig eine nicht mehr funktionierende Installation zurücksetzen und den Inbetriebnahme-Prozess (#5) wieder neu starten.

Der Austausch eines Devices kann ohne die Interaktion der IT erfolgen. Sobald der Benutzer das neue Device erhalten hat kann er wieder den Inbetriebnahme-Prozess (#5) starten.

Die Ausserbetriebnahme benötigt keine nachgelagerten Datenlöschprozesse, da alle eingesetzten Festplatten verschlüsselt sind.

3.3 Voraussetzungen Netzwerk

Damit die in den vorherigen Kapiteln beschriebene Lösung korrekt und performant arbeiten kann müssen die folgenden Rahmenbedingungen erfüllt sein:

1. LAN

- a. Ausschliessliche Verwendung von verwaltbaren Aktivkomponenten, welche die logische Trennung Schulbetrieb, Verwaltung und Gastbetrieb (VLAN) korrekt unterstützen
- b. **Physischer Schutz:** Die Aktivkomponenten und die physischen LAN-Anschlüsse dürfen nicht öffentlich zugänglich sein. Falls sich dies nicht verhindern lässt (öffentliche LAN-Dosen, welche mit dem internen LAN verbunden sind) muss über den Einsatz einer NAC Lösung (siehe unten) nachgedacht werden.
- c. **Port Bandbreite:** 1 Gbit/s oder höher
- d. **Verkabelung:** UKV Cat 5e oder besser
- e. **Verfügbarkeit** Der Grad der LAN-Verfügbarkeit innerhalb der definierten Betriebszeiten muss in der Service Beschreibung festgelegt werden

2. WLAN

- a. **Abdeckung / Use Cases:** Abdeckungsgrad an den festgelegten Örtlichkeiten und den zu erwartenden Use Cases (wie viele User/Devices gleichzeitig und welche Aktionen/Arbeiten werden prioritär ausgeführt).
- b. **Verfügbarkeit:** Der Grad der WLAN-Verfügbarkeit innerhalb der definierten Betriebszeiten muss in der Service Beschreibung festgelegt werden.
- c. **Performance:** Die WLAN-Komponenten müssen die geforderte Geschwindigkeit und Bandbreite für die festgelegten Use Cases nachweislich erbringen.
- d. **Sicherheit:** Die WLAN-Komponenten müssen auf der Transportebene eine State-of-the-Art Verschlüsselung (aktuell WPA2 → AES) bereitstellen.
- e. **Authentifizierung und Autorisierung:** Der Benutzer und das Device müssen berechtigt sein eine «interne» WLAN-Verbindung aufzubauen. Für unbekannte Devices muss der Benutzer die Möglichkeit haben eine «Internet-only» WLAN-Verbindung über ein Captive Portal aufzubauen (SMS).
- f. **Standards:** Unterstützung aller aktuell freigegebenen Wi-Fi Standards
- g. **Verwaltung:** Cloud basierte Verwaltung

3. Internet und Firewall

- a. **Performance:** Der Internetzugang sollte mit dem höchstmöglichen Geschwindigkeits-Profil betrieben werden, welche vom Provider zur Verfügung gestellt wird. Es wird eine synchrone Bereitstellung (Download Speed = Upload Speed) empfohlen. Empfohlene mind. Bandbreite pro Standort siehe Kapitel 2.7.3 *Netzwerk*
- b. **Verfügbarkeit:** Der Grad der Internet Verfügbarkeit innerhalb der definierten Betriebszeiten muss in der Service Beschreibung festgelegt werden. Es wird empfohlen zwei Internetanschlüsse von unterschiedlichen Providern im aktive/aktive Modus zu betreiben. Im Weiteren sollten ebenfalls zwei Firewalls im aktive/aktive Modus die Internet-Connectivity zur Verfügung stellen.
- c. **Next Generation Firewalls (NGFW):** Es wird der Einsatz einer Next Generation Firewalls (NGFW) empfohlen. Dabei handelt es sich um Sicherheitslösungen, die über die Protokoll- und Port-Inspection klassischer Firewalls hinausgehen und Datenanalysen auf Anwendungsebene ermöglichen.
- d. **Malware Schutz:** Die Firewalls müssen einen aktuellen Malware Schutz für den gesamten eingehenden Internetverkehr bereitstellen. Zusätzlich werden weiterführende Firewall integrierte Schutzmassnahmen empfohlen wie etwa Application Control oder Advanced Threat Protection (ATP) Lösungen.
- e. **Content Filter:** Die Firewall muss einen aktuellen Content Filter für den gesamten eingehenden Internetverkehr bereitstellen.

Hinweis:

Die eingesetzten Firewalls müssen, die vom Provider zur Verfügung gestellten Bandbreiten unterstützen! Im Weiteren müssen die Firewalls genügend Rechenleistung bereitstellen um sämtliche Zusatzservices (Antivirus, ATP, etc.) ohne nennenswerte Performance Einbussen zu betreiben.

Wichtig:

Für den gesamten Office 365 Traffic muss ein direkter Zugriff (keine Proxys, Malware Filtering oder sonstige Security-Applikationen) zu den entsprechenden Microsoft Cloud Services sichergestellt werden.

4. Betrieb und Support

Im Betrieb müssen folgende Punkte beachtet und definiert werden:

- Backup, Restore und Verfügbarkeit
 - Die Datensicherung von Office 365 muss bei einem externen Anbieter erfolgen. Nur so können Daten jederzeit wiederhergestellt werden. Wir empfehlen ein Enterprise Cloud to Cloud Backup, beispielsweise bei Green.ch. Die Kosten fallen aufgrund der gewünschten Datenmenge an.
 - Die Verfügbarkeiten der einzelnen Systeme sind zu eruieren: Internet-Provider, Cloudanbieter: In der Regel haben diese hohe Verfügbarkeiten.
- Die Bewirtschaftung der Cloud soll in Zusammenarbeit mit dem externen Partner erfolgen: Einfache Aufgaben (Benutzerverwaltung, Recovery, Schnittstelle zum Schulinformationssystem) kann durch den 1st Level erfolgen. Struktur Anpassungen (Datenablage, Features und Berechtigungen) soll durch den externen Dienstleister erfolgen.
- Die 1:1 SuS od. LP Endgeräte werden bei Schulaustritt zurückgegeben und der externe Dienstleister wird diese Endgeräte wiederaufbereiten (Reset). Für die Masse an jährlichen Ein- und Austritten soll der externe Dienstleister beigezogen werden. Kleinere unterjährliche Slots könnte durch den 1st Level Support erledigt werden.
- Pro-Aktives Monitoring: Aufgrund der Entwicklung in der Nutzung kann in einem Monitoring festgestellt werden, ob bestimmte Aufgaben planbar umgesetzt werden müssen:
 - Security und Update -Tasks für den MDM-Bereich
 - Office 365 Compliance und Security
- Die Weiterentwicklung der Cloud-Infrastruktur ist ein wesentlicher Teil, da diese sehr rasch an neuen Funktionen und Updates hervorbringt in allen Bereichen:
 - Security
 - Neue Anforderungen der Schule (Strukturen, Features, Applikationen / Apps, usw.)
- Prozesse; Die Einbindung oder Anbindung von Daten/Informationen in die IT-Architektur soll fortlaufend geprüft werden, zum Beispiel die Schuldatenbank. Mit der synchronisierten Übernahme von einfachen (nicht schützenswerten) Benutzerdaten für die Verarbeitung zur Anmeldung/Autorisierung an der Schul-IT.
Beispielsweise: LehrerOffice/Solaris werden zur Anmeldung, Benutzerinformationen synchronisiert oder Datenstrukturen und Berechtigungen in der Cloud angelegt. Verschiedene Schulapplikationen oder Schulwebsites werden zukünftig mit Edulog (www.edulog.ch - schützt die digitalen Identitäten im Bildungsraum Schweiz) fördern, dies als Chance die bekannten Schnittstellen anzubinden.

Aufwendige oder repetitive administrative Aufgaben sollen vermehrt automatisiert und standardisiert werden, um den Betrieb zu standardisieren (effizienter) und den Supportaufwand zu verringern.

- SLA (*Kapitel 4.5*); Es muss mit allen Leistungserbringern einen Rahmenvertrag zwischen Auftraggeber (Kreisschule Aarau-Buchs) und internen/externen Dienstleister für wiederkehrende Dienstleistungen, Support, Reaktionszeiten und Betrieb, vereinbart werden. Dieses Modell muss innerhalb der internen Schulstruktur definiert werden, um die Erwartungshaltungen der Endanwender im Betrieb und Support zu deklarieren. Bei externen Partnern werden die Leistungen, Reaktionszeiten, und Zeitraum definiert und die entsprechenden Konditionen ausgehandelt.

4.1 Organisation

Die Lösung zielt aufgrund einer homogenen Systemarchitektur, Nutzung von Cloud-Ressourcen (inkl. Verwaltung der Endgeräte) und eine einheitliche Endgerätewahl auf einen organisierten und strukturierten Betrieb und Support. Es soll zu Beginn, Klarheit über die Leistungserbringer und internen und externen Aufgaben/Kernkompetenzen, sowie die damit verbunden Serviceleistungen geschaffen werden:

- Mit der Nutzung von Cloud sind klare Verfügbarkeiten und Sicherheiten definiert und durch die IT-Administration und den Support geregelt (Nutzungsagreement Cloud-Provider).
- Mit der Beschaffung von Endgeräten werden Garantieleistungen und Prozesse vereinbart (DOA & RMA -> Austausch und Reparatur).
- Zur Basis-Infrastruktur gehört ein professionelles Netzwerk, Zugriffs- und Sicherheitskonzept, sowie die notwendigen Internet-Provider. Der Betrieb und der Support werden dediziert geregelt.

Aufgrund der kantonalen Vorgabe und schulinternen Kompetenzen sollen die im nachfolgenden Kapitel genannten Aufgaben im «technischen 1st Level Support» und «pädagogischen Support» durch die Schule erbracht werden.

4.2 Steuerung und Support

Eine Neukonzeption der Kapitels 4.2 bis 4.4. wird aktuell in einem Organisationskonzept erarbeitet, da der externe technische Support durch Entscheid der Kreisschulpflege vom 20. Januar 2021 der IZAB zugewiesen wird.

Inhaltlich werden im Organisationskonzept folgende Themen geregelt:

- *Beschreibung der Steuerungsgremien und Definition der Zuständigkeiten*
- *Beschreibung pädagogischer und technischer Support und der Betriebsabläufe*
- *Vorgaben für die Nutzung der ICT-Mittel für SuS, LP und Verwaltung*

Die strategischen Themen bezüglich Weiterentwicklung und Betrieb (Support) der Schulinformatik sollen in den einzelnen Gruppen, zusammen mit den Schulleitungen und den Leistungserbringern (Support), besprochen und entschieden werden. Die Gruppen haben klare Aufgaben zu erfüllen und sollen den zukünftigen Anforderungen im Schulumfeld gerecht werden.

ICT-Kerngruppe

Die Geschäftsleitung, die Leitung Dienste und die Leitung Informatik legen in Zusammenarbeit mit der Kreisschulpflege die mittel- und langfristigen Ziele zur medienbezogenen Weiterentwicklung der Schule fest. Sie beschliesst die langfristige Ressourcenplanung.

ICT-Steuergruppe

Die ICT-Steuergruppe setzt sich zusammen aus der Geschäftsleitung, der Leitung Dienste, dem Leiter Informatik einer Schulleitung jeder Schulstufe und aus den Mitgliedern des technischen Supports.

Die ICT-Steuergruppe wird geleitet von einem Mitglied der Geschäftsleitung. Die Steuergruppe konstituiert sich selbst.

Die Aufgaben sind:

- Aufnehmen von Entwicklungen im Bereich Medien und Informatik
- Vorbereiten und Beantragen von richtungsweisenden Entscheiden bei der GL

- Gewährleisten der Einhaltung des Datenschutzes und der Datensicherheit
- Konzipieren und Planen der Weiterbildung der Schulleitungen und der Lehrpersonen im Bereich Medien & Informatik
- Umsetzen des ICT-Konzepts sowie der von der GL vorgegebenen Ziele
- Planen der Beschaffung und des Einsatzes der IT-Infrastruktur (Hardware und Software)

Die Leitung Informatik führt die Mitarbeitenden des technischen Supports.

Die ICT-Steuergruppe trifft sich 4 bis 6 Mal pro Jahr. 2 Mal jährlich treffen sich alle Mitglieder der ICT-Steuergruppe, des technischen sowie des pädagogischen Supports.

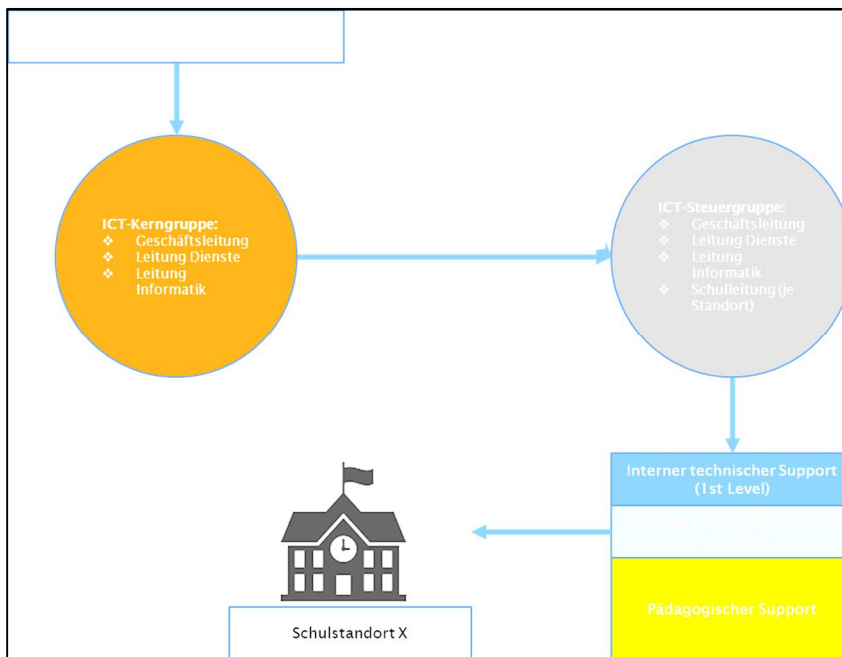


Abbildung 8 Steuerung und Support

Technischer Support

a) Interner technischer Support (1st Level)

Der interne technische Support setzt sich aus der Leitung ICT Technik und einer weiteren Person zusammen, so dass die Stellvertretung sichergestellt ist, das Knowhow gesichert werden kann und zwei Ansprechpersonen insbesondere in hektischen Zeiten zur Verfügung stehen. Mit der wachsenden Anzahl Schülerinnen und Schülern sowie zunehmender technischer Ausstattung muss der technische Support ausgebaut werden.

Die beiden Personen stellen den Support an 5 Arbeitstagen von 07.30 bis 17.00 Uhr sicher. Die Lehrpersonen und Schulleitenden lösen bei Problemen ein Ticket beim technischen Support. Dieser nimmt entweder per Telefon Kontakt auf oder geht zur Problembehebung vor Ort. Der technische Support ist zentral organisiert und hat sein Büro inkl. Lagerraum in der Geschäftsstelle der KSAB.

Die Aufgaben sind:

- Anlaufstelle für alle technischen Fragen und Probleme aus den Schulhäusern
- Zentraler Einkauf der Soft- und Hardware
- Gerätedienst für alle Schulhäuser
- Auftraggeber für externe Aufträge (Partner) gemäss Vorgaben der Steuergruppe
- Beratung der ICT-Steuergruppe
- Zusammenarbeit mit dem pädagogischen Support und mit den Schulleitenden
- Sicherstellen einer jederzeit aktuellen Dokumentation (Inventar, Datenbanken, Archiv, Lizenzen, Passwörter etc.)

- Administration Teams/SharePoint (Office 365) und LehrerOffice (Klassenverwaltungsprogramm mit Zeugnissoftware)
- Melden und Vorstellen von Neuanschaffungen an die ICT-Steuergruppe

Die Aufgaben sollen in einem Pflichtenheft konkretisiert werden (Beispielsweise in einem Stellenbeschrieb TICTS).

b) *Externer technischer Support (2nd & 3rd Level)*

Nebst dem internen technischen Support ist ein externer Support notwendig, da nicht alle Supportprobleme intern gelöst werden können.

Die Aufgaben sind:

- Unterstützung im Unterhalt von Cloud Services (Office 365), Endgeräten (MDM) und Peripherie
- Unterhalt der Netzwerkinfrastruktur (ev. weitere Serviceprovider)
- Support bei Störungen sowie allgemeine Beratung und Weiterentwicklung
- Backup/Restore Office 365

Ergänzung: Entwurf des Kapitels "Technischer Support" aus dem Organisationskonzept

Support

Lehrpersonen sowie Schülerinnen und Schüler der KSAB erhalten durch den technischen und den pädagogischen Support Unterstützung in der Nutzung der vorhandenen ICT-Mittel. Zur besseren Unterscheidung des technischen und des pädagogischen Supports werden nachfolgend die Begriffe «technischer Support» und «pädagogische ICT-Beratung» verwendet.

Unterscheidung

Technischer Support	Pädagogische ICT-Beratung
<i>ICT ist verfügbar und funktioniert</i>	<i>Pädagogisch-didaktische ICT-Nutzung</i>
<i>Der technische Support ist für die Beschaffung und die Funktionstüchtigkeit der ICT-Mittel inkl. Peripherie zuständig.</i>	<i>Die pädagogische ICT-Beratungsperson bietet Beratung und Unterstützung an, wie man zielgerichtet den Unterricht mit ICT-Mitteln gestaltet.</i>

Technischer Support

Der technische Support wird mit einem internen technischen Support (TICT) und dem externen technischen Support sichergestellt.

Aufgaben interner technischer Support (TICT)

- Drucker: Toner auffüllen, wechseln, reinigen, Papierstau entfernen
- Defekte Tastaturen und Mäuse ersetzen
- Verwaltung Lernplattformen auf Ebene Schulhaus
- Ausleihe und Pflege von weiteren Informatikmitteln im Schulhaus (Beamer, Kameras...)
- Technische Einführung neuer Lehrpersonen

Aufgaben externer technischer Support

- Anlaufstelle für alle technischen Fragen und Probleme aus den Schulhäusern (inkl. Peripherie)
- Zentraler Einkauf der Soft- und Hardware
- Gerätedienst für alle Schulhäuser (inkl. Peripherie)
- Drucker: Zentrale Bestellung und Verwaltung Toner

- *Auftraggeber für externe Aufträge (Partner) gemäss Vorgaben der Steuergruppe*
- *Beratung der ICT-Steuergruppe*
- *Zusammenarbeit mit dem pädagogischen Support und mit den Schulleitenden*
- *Sicherstellen einer jederzeit aktuellen Dokumentation (Inventar, Datenbanken, Archiv, Lizenzen, Passwörter etc.)*
- *Melden und Vorstellen von Neuanschaffungen an die ICT-Steuergruppe*
- *Unterstützung im Unterhalt von Cloud Services (Office 365), Endgeräten (MDM) und Peripherie*
- *Unterhalt der Netzwerkinfrastruktur*
- *Support bei Störungen sowie allgemeine Beratung und Weiterentwicklung*
- *Backup/Restore Office 365*

Pädagogischer Support

Der pädagogische Support setzt sich aus der Leitung ICT Pädagogik und je einer Lehrperson, die selbst auch unterrichtet, aus jedem Schulhaus zusammen (für kleinere Teams können Ausnahmen gelten). Die Mitglieder des pädagogischen Supports verfügen über das entsprechende Stufendiplom sowie über den Zertifikatslehrgang CAS «PICTS».

Der pädagogische Support trifft sich einmal pro Quartal für einen Austausch.

Die Aufgaben sind:

- *Beratung und Schulung von Lehrpersonen und Schulleitenden in pädagogischen Fragen im Bereich Medien & Informatik*
- *Kennen der Trends und Entwicklungen im pädagogischen Bereich Medien & Informatik*
- *Initiieren und allenfalls Durchführen von Weiterbildungsanlässen in den Schulhausteams*
- *Impulse geben für die Unterrichtsentwicklung*
- *Zusammenarbeit mit dem technischen Support und mit den Schulleitenden*
- *Melden und Vorstellen von Neuanschaffungen an die ICT-Steuergruppe sowie an die Schulleitungen (zur Prüfung und Planung des Weiterbildungsbedarfs)*

Die Mitglieder des pädagogischen Supports werden von den Schulleitenden des jeweiligen Schulhauses personell geführt. Die Aufgaben sollen in einem Pflichtenheft konkretisiert werden (Beispielsweise in einem Stellenbeschrieb PICTS).

Ergänzung: Neubetrachtung im pädagogischen ICT-Konzept

4.3 Kalkulatorischer Aufwand PICTS

- Der kalkulatorische Aufwand für die pädagogische Beratung ist aktuell in Bearbeitung, da die Kosten über den Ressourcenpool der KSAB getragen werden sollen. Diese Neuberechnung ersetzt Kapitel 4.3.1 bis Kapitel 4.4.4

4.3.1 Entschädigungsmodell pro Endgerät

Dieses Modell bezieht sich auf die Anzahl Endgeräte an der Schule und stellt einen festen Betrag pro Endgerät pro Jahr ein. Je grösser die Anzahl der Endgeräte an einer Schule ist, desto seriöser und geringer wird dieser Betrag. Die ursprüngliche Modell-Kalkulation hat sich auf eine kleinere, und mittlere Schule bezogen. Wir gehen in diesem technischen Konzept davon aus, dass eine hohe Standardisierung, homogener Gerätepark und moderne Mittel eingesetzt werden.

Berechnet wird über den zu erwarteten Betrag für den ganzen Support, aufgeteilt auf die interne und externe Unterstützung.

Ansatz: Fr. 100.- bis 150.- pro Endgerät und Jahr rechnen, Schule > 2000 Geräte		
Verteilung der Stunden von 3:1 zu Gunsten der päd. ICT-Beratung: 75% Intern / 25% Extern		
Weitere Grundlage ist, dass eine Jahreslektion mit Fr. 3900 entschädigt wird.		
Anzahl Endgeräte	Betrag pro Endgerät	Total
2364	Fr. 100.00	Fr. 236'400.00

Tabelle 20 Grundlagen Entschädigungsmodell pro Endgerät

	Lektionen/Jahr	Modell 75% Intern (umverteilt) / 25% Extern
Fr. 157'600.00	÷ 3900	66.7% Pädagogischer Support
	40.5	
Fr. 19'700.00	÷ 3900	8.3% Interner technischer Support (1st Level)
	5.1	
(Fr. 59'100.00)	-	25.0% Externer technischer Support (2nd & 3rd Level)
	-	
Fr. 236'400.00		
	45.6	Pädagogischer und interner technischer Support (1st Level)

Tabelle 21 Berechnung Entschädigungsmodell pro Endgerät

4.3.2 Empfehlung

Für den pädagogischen, sowie internen technischen Support soll zu Beginn genügen Ressourcen budgetiert werden. Das Modell pro SuS vernachlässigt die hohe Anzahl Endgeräte und vernachlässigt die LP in der Berechnung. Das Modell pro Endgerät, geht davon aus, dass jeder Anwender (LP, SuS) ein schuleigenes Gerät verwendet, um die Erfüllung der Tätigkeiten in nachzukommen und sie hinsichtlich dieser Nutzung entsprechende Unterstützung benötigen.

Fazit: Es soll mit dem Ansatz von **46 Jahreslektionen** den schulinternen Support geregelt werden. Dies entspricht einem Pensum von ca. 164% Stellenprozent, verteilt auf das ganze Support-Team. Die interne Umverteilung (pädagogisch/technisch) kann situativ definiert werden.

4.4 Berechnungsgrundlagen Betrieb und Support (extern)

In der Cloud-Ausprägung sind die Betriebs- und Supporttätigkeiten im 2nd und 3st -Level Support mit Schwerpunkt MDM und Office 365 gelagert. Es soll aus Erfahrungen und Referenzen in dieser Grössenordnung eine seriöse Messgrösse zur Budgetierung festgelegt werden. Diese basiert nicht auf die Anzahl Benutzer, sondern auf die Anzahl Endgeräte. Dies ist eine messbare Grösse, gerade in einer IT-Umgebung mit einer hohen Anzahl von Endgeräten in einer professionellen Infrastruktur. Kostentreiber wie Redundante-Serversystem, konventionelle Backups und Sicherheiten entfallen und verlagern sich in die skalierbare Cloud.

Alle Angaben gehen von einer hohen Verfügbarkeit und Ausfallsicherheit der Basisdienste und Komponenten im Netzwerkbereich aus: Internetprovider, Firewall (inkl. Contentfilter), physisches und drahtloses Netzwerk (inkl. Security).

Aus heutiger Erfahrung und Annahmen wird der Betrieb mit den folgenden Punkten sichergestellt:

- Externer Support 2nd & 3rd: Office 365 und MDM
- Support Bereitschaft; SLA (Service Level Agreement), Support und garantierte Reaktionszeiten
- Pro-Aktive Betriebsaufgaben: Monitoring, Backup, Security und Update -Tasks: Office 365 und MDM
- Consulting (Technik); Beratung und Weiterentwicklung der Infrastruktur
- Festgelegte Aufgaben; Endgeräte / Reset (jährliche Wiederaufbereitung der SuS 1:1 Convertible)
- Hohe Verfügbarkeit der Cloud Services 99.9%
- Sicherungen (Backup) der Office 365 Umgebung
- Helpdesk-Tool

Die betrieblichen Aufwendungen und Beschreibung stehen in der Anlage zur Verfügung:

ICT-Konzept KSAB Berechnung Investition und Betrieb.xlsx

➔ Zeilen: *Externe Betriebs- und Supportkosten* und *Fortführende Investitionen*

Zur Berechnung des Support-Aufwandes wurden verschiedene Geräte-/Nutzertypen festgelegt, die in diesem Konzept ein entsprechendes Endgerät erhalten, in der Berechnung wurde ein Sockel-Aufwand für die ersten 100 Endgeräte festgelegt. Der errechnete Aufwand reduziert sich pro weiteren 50 Geräten prozentual. Es resultiert in der Vereinfachung ein Durchschnittswert an Aufwand pro Gerät. Detaillierte Angaben stehen in der Anlage zur Verfügung: **ICT-Konzept KSAB Berechnung Support.xlsx** im Register [Supportberechnung]

4.4.1 Modell pro Endgerät (*Neuberechnung durch IZAB*)

Die vier Typen sind:

<p>Verwaltete "shared" Endgeräte 1:n mit Office 365 OS: iOS / Typ: Tablet</p> <p style="text-align: center;">Grundlage/Aufwand pro Gerät/Jahr: 0.25[h]</p> <p><i>Bemerkung: Hohe Standardisierung und grosse Anzahl an verwalteten Endgeräten, die mehreren Anwendern zur Verfügung gestellt werden. Bedingt durch den Gerätetyp, die Nutzung und der Anwendergruppe ist hier mit geringerem Aufwand zu rechnen.</i></p>
<p>Verwaltete "shared" Endgeräte 1:n mit Office 365 OS: Windows / Typ: Convertible, Notebook</p> <p style="text-align: center;">Grundlage/Aufwand pro Gerät/Jahr: 0.50[h]</p> <p><i>Bemerkung: Hohe Standardisierung und grosse Anzahl an verwalteten Endgeräten, die mehreren Anwendern zur Verfügung gestellt werden. Es können individuelle technische Anwenderproblemstellungen durch die unterschiedliche Nutzung der Endgeräte entstehen.</i></p>
<p>Verwaltete persönliche Endgeräte 1:1 mit Office 365 OS: Windows / Typ: Convertible, Notebook</p> <p style="text-align: center;">Grundlage/Aufwand pro Gerät/Jahr: 0.33[h]</p> <p><i>Bemerkung: Hohe Standardisierung und grosse Anzahl an verwalteten Endgeräten.</i></p>
<p>Unverwaltete persönliche Endgeräte BYOD mit Office 365 (Ausstattung: nur LP)</p> <p style="text-align: center;">Grundlage/Aufwand pro Gerät/Jahr: 0.75[h]</p> <p><i>Bemerkung: BYOD darf nicht unterschätzt werden bezüglich Supportaufwand, gerade aufgrund unterschiedlicher Ausprägungen und Voraussetzungen der Endgeräte, sowie die Anwenderkenntnisse in Bezug auf Office 365 und deren Geräte- Integration, Installation und Konfiguration.</i></p>

Tabelle 22 Geräte-/Nutzertypen

4.4.2 Zusammenfassung der Berechnung

Kalkulierter Aufwand pro Typ / Jahr	Aufwand [h] pro Gerät/Jahr	Anzahl Geräte	Summe [h]
Verwaltete "shared" Endgeräte 1:n mit Office 365 OS: iOS / Typ: Tablet	0.20	340	68.50
Verwaltete "shared" Endgeräte 1:n mit Office 365 OS: Windows / Typ: Convertible, Notebook	0.42	579	242.65
Verwaltete persönliche Endgeräte 1:1 mit Office 365 OS: Windows / Typ: Convertible, Notebook	0.23	1380	312.33
Unverwaltete persönliche Endgeräte BYOD mit Office 365 (Ausstattung: nur LP)	0.75	65	48.75
	Total	2364	672.2

Tabelle 23 Supportaufwand (2nd/3rd Level)

4.4.3 Empfehlung

- Es soll für den **externen Support 700 Stunden/Jahr** berechnet werden.

Dieser externe Aufwand wurde jeweils im TCO berücksichtigt!

4.4.4 Gegenüberstellung IST-SOLL (Konzept)

Es wird nach Abschluss dieses Konzeptes eine Gegenüberstellung der heutigen und zukünftigen Betriebs- und Supportaufwendungen erarbeitet.

4.5 SLA

Wir empfehlen eine Vereinbarung mit den Endkunden (Anwender der Kreisschule Aarau-Buchs und IT-Verantwortliche der Schule) um die gewünschten Services und erwartenden Reaktionszeiten, vor allem im Support zu definieren.

Ein wichtiger Aspekt sind die Begriffsdefinitionen im SLA / Support in nachfolgender Abbildung:

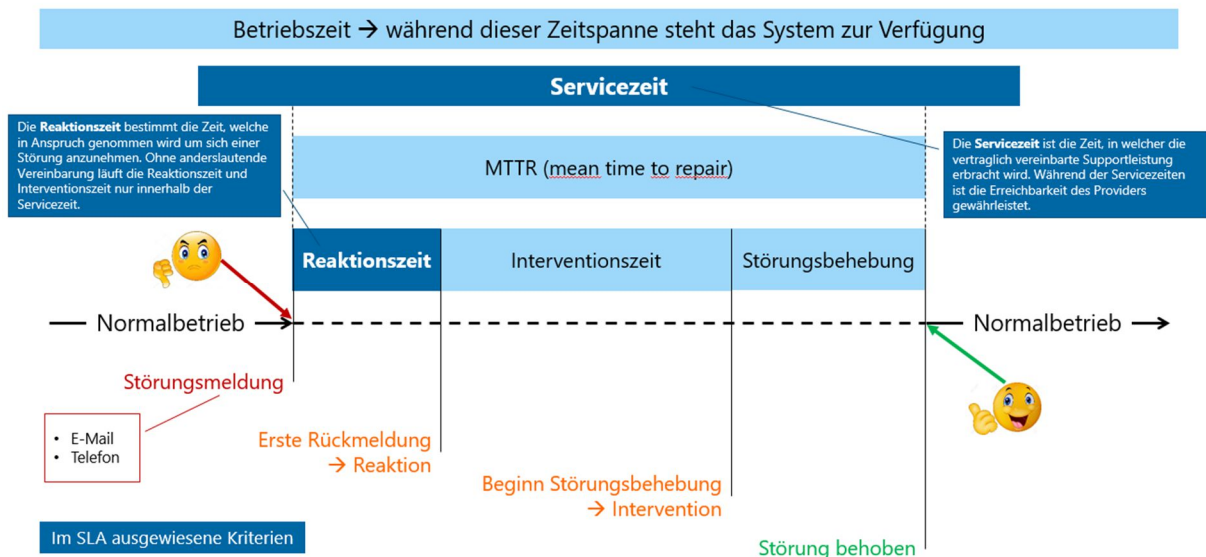


Abbildung 9 SLA / Support, Begriffsdefinitionen

Mit der Einführung einer Cloud-only Lösung, MDM und Office 365 stehen diese Dienste, allen Anwendern rund um die Uhr zur Verfügung, unabhängig ob sie in der Schule oder von Ausserhalb darauf zugreifen und nutzen. Somit kann von einer hohen **Betriebszeit 7 x 24h** ausgegangen werden.

Die Servicezeit ist die Zeit, in welcher die vertraglich vereinbarte Supportleistung erbracht wird. Während der Servicezeiten ist die Erreichbarkeit des (internen/externen) Supportdienstleisters gewährleistet.

MTRR: Ist die mittlere Reparaturzeit nach einem Ausfall eines Systems und soll so kurz wie möglich gehalten werden.

Die Reaktionszeit bestimmt die Zeit, welche in Anspruch genommen wird, um sich einer Störung anzunehmen. Ohne anderslautende Vereinbarung läuft die Reaktionszeit und Interventionszeit nur innerhalb der Servicezeit.

Empfehlung an einen externen Support-Dienstleister:

Generelle Servicezeiten	Werktags zwischen 08:00 und 17:00 Uhr Es gelten die Feiertage des Kantons Aargau
Reaktionszeiten Support	Für reguläre Meldungen längstens 1 Tag nach Eingang
Pikett (Störungsmeldung)	Kein Pikettdienst
Schulbetrieb	Die Betriebs- und Supportorganisation des externen Partners ist während den Schulzeiten und den Schulferien zu gewährleisten.
Störungsmeldung	Über ein Ticketing des Partners, per Email oder Telefon

Zur Berechnung und aus Erfahrung haben wir eine fixe Monatspauschale (Mindestlaufzeit von 12 Monaten) zur Sicherstellung des 2nd & 3rd -Level Supports und deren garantierten Reaktionszeiten hinterlegt.

Diese Pauschale kann variieren und je nach erweiterten Aufgaben, anderen Servicezeiten, beispielsweise: 1st-Level Support mit erhöhten Reaktionszeiten, Ferien-Stellvertretungen der PICTS im technischen Support, usw.

5. Datensicherheit und Datenschutz

Datensicherheit

Der neue Leitfaden Office 365 in Volks-, Mittel- und Hochschulen des Datenschutzbeauftragten Kanton Zürich bietet eine detaillierte Anleitung zum datenschutzkonformen Einsatz von Office 365. Educa.ch hat mit Microsoft einen Rahmenvertrag für die Nutzung von Office 365 auf Primar- und Sekundarstufe und Switch einen solchen für die Hochschulstufe unterzeichnet. geregelt werden darin rechtliche Aspekte wie das anwendbare schweizerische Recht und der schweizerische Gerichtsstand. Microsoft verpflichtet sich, die Daten in europäischen Ländern zu speichern.

Für Bildungseinrichtungen unter dem educa.ch-Rahmenvertrag erfolgt die Beitrittserklärung, indem ein Microsoft-Volumenlizenzvertrag unterzeichnet wird, der beim für die Schule zuständigen Microsoft Authorized Education Partner erhältlich ist. Die Schule muss explizit darauf hinweisen, dass eine Beitrittserklärung unter Inanspruchnahme des educa.ch-Rahmenvertrags gewünscht wird, sonst kommen die speziellen datenschutz-rechtlichen Rahmenbedingungen nicht zum Tragen. Der Einsatz von Office 365 kann sich am Leitfaden des Kantons Zürich richten. <https://dsb.zh.ch/dam/dsb/publikationen/leitfaeden/Leitfaden-Office-365-in-den-Schulen.pdf>

Datenschutz

Es ist wichtig, insbesondere die Personendaten von Schülerinnen und Schülerin sowie den Lehrpersonen zu schützen. Nebst den allgemeinen Personendaten (z.B. Personalien) geht es auch um besonders schützenswerte Personendaten. Es handelt sich dabei um Angaben über religiöse, weltanschauliche oder politische Ansichten, die Gesundheit, die Intimsphäre sowie die ethnische Zugehörigkeit, Massnahmen der sozialen Hilfe sowie allfällige Straftaten. Zum Umgang mit Personendaten an öffentlichen Schulen ist ein kantonaler Leitfaden geplant. Wichtige Hinweise für Lehrpersonen und Schulleitungen bietet der «Leitfaden Datensicherheit für Lehrpersonen und Schulleitungen» des Dachverbands Lehrerinnen und Lehrer Schweiz (LCH). https://www.lch.ch/fileadmin/files/documents/Verlag_LCH/Leitfaden_Datensicherheit_Web_DEF.pdf

6. Gesamtkostenbetrachtung (TCO – 5 Jahre)

Die finale Kostenaufstellung wird aus den aktuell laufenden Abstimmungen mit dem externen Dienstleister basieren, welcher sich an den Vorgaben dieses Konzepts orientiert. Wichtig ist festzuhalten, dass die aktuell geplant stärkere Auslagerung von Supportleistungen an den Externen, und die Übernahme des jetzigen Netzwerkbetriebs und der aktuellen Peripherie vom externen Dienstleister, für einen Betrieb und Support aus einer Hand, bei der Erstellung des Konzeptes durch die Netree AG noch nicht in die Kostenaufstellung miteingerechnet wurde. Der finale Kreditantrag wird dem Kreisschulrat jedoch transparent zur Beschlussfassung vorgelegt.

Die Gesamtkostenbetrachtung schätzt die anfallenden Investitions-, Projekt, Betriebs- und Supportkosten ab. Sie bezieht sich auf das definierte Mengengerüst in der Beschaffung von Endgeräten, Zubehör und Aufbewahrung, die notwendigen Projektdienstleistungen (inkl. Migration und Rollout), den Betrieb- und Supportaufwand eines externen Dienstleisters für den definierten Support-Level, sowie die Nutzungskosten von Software und Cloud Services.

Nicht berücksichtigt in der TCO-Betrachtung:

- Ist das Netzwerk (Investition, Betrieb und Support)
- Die Personalkosten der Schule für den pädagogischen Support
- Die Kosten für Fach- und Schulapplikationen (ausgenommen Office 365 ProPlus)
- Externe Beratung und Unterstützung in der Ausschreibung (ICT-Konzept)
 - Je nach Submissionsverfahren: öffentliche Ausschreibung mit oder ohne Vorselektion der Anbieter
 - Pflichtenheft und Ausschreibungsunterlagen (Anforderungen, Eignungs- und Zuschlagskriterien) erstellen
 - Publikation Fragen/Antworten, Auswertung und Entscheid
- Gesamtprojektleitung Umsetzung (ICT-Konzept)
- Weitere in diesem Konzept nicht genannten schulinterne Ausgaben für IT oder IT nahe Themen (beispielsweise die Peripherie)

Zur Berechnung des TCO

Alle Grundlagen haben den Stand Februar 2020 und die Preise sind in Schweizer Franken, inklusive der aktuellen Mehrwertsteuer von 7.7%.

Die Berechnung «Investition und Betrieb» besteht aus nachfolgenden Positionen

Beschreibung	Intervall	Ergänzung
Hardware Beschaffung	Einmalig Investition	Bei der Beschaffung werden die beiden Varianten berechnet. In der Regel wird einmalig beschafft.
Projektkosten (Dienstleistungen)	Einmalig Investition	Dienstleistungen durch Dritte / Externe Dienstleister (Annahmen und Erfahrungswerte)
Nutzungskosten Azure Office365	jährlich wiederkehrend	Mit den erweiterten Sicherheitsfunktionen für den Datenschutz und die Datensicherheit für besonders schützenswerte Personendaten in der Cloud und erhöhte Verschlüsselung zwischen Anwender und der Cloud Ressourcen.
Externe Betriebs- und Supportkosten	jährlich wiederkehrend	Die Grundlage besteht aus verschiedenen Erfahrungswerten und Annahmen von ähnlich gelagerten Schulinformaticklösungen, mit der Cloud-only Strategie.

Fortführende Investitionen	wiederkehrend ab 2. Betriebsjahr	Zu berücksichtigen sind: Geräteersatz, jährliche Neubeschaffungen aufgrund der angepassten SuS-Zahlen oder zwischenzeitlich notwendig zu ersetzenden Geräten.
----------------------------	----------------------------------	---

Tabelle 24 Kurzbeschreibung TCO-Positionen

Die Geräteausstattung teilt sich auf die einzelnen Schulstufen auf. In der Berechnung wurden die bestehenden Geräte berücksichtigt (*Tabelle 18 Lebenszyklen der bestehenden Endgeräte*), das heisst diese müssen vorerst nicht neu beschafft, sondern zu einem späteren Zeitpunkt ersetzt werden, dazu ist ein Investitionsbetrag in den «Fortführende Investitionen» hinterlegt.

Stufe	Tablet	Convertible/ Notebook
Kindergarten	60	
Primarschule 1. - 3. Klasse	280	
Primarschule 4. - 6. Klasse		497
Oberstufe		20
LP 1:3		62
Oberstufe		1120
LP 1:1		260
LP [BYOD]		65
Anzahl Geräte		2364

Tabelle 25 Anzahl Geräte

Die detailliert Berechnungsgrundlage und Beschreibung stehen in der Anlage zur Verfügung, Dokument: **ICT-Konzept KSAB Berechnung Investition und Betrieb.xlsx**

In den folgenden Registern sind: [InvestBetriebskosten] (Investitions- und Betriebskosten - Detailkalkulation [Nutzungskosten Azure Office365], [TCO], [5YHW] (Endgeräte Lebenszyklus), [Erfahrungsreferenz].

6.1 Berechnung TCO

Kurzbeschreibung:

- Die Beschaffung aller Endgeräte SuS wird durch die Kreisschule Aarau-Buchs finanziert.
- 100% aller Endgeräte für LP werden durch die Kreisschule Aarau-Buchs finanziert.
- Es werden die Erweiterten-Nutzungslizenzen berechnet.

		Total / 5 Jahre
Hardware Beschaffung	einmalig Investition	Fr. 2'167'095.00
Projektkosten (Dienstleistungen)	einmalig Investition	Fr. 252'105.00
Nutzungskosten Azure Office365 II (Lizenzen inkl. Advanced Security)	jährlich wiederkehrend	Fr. 358'937.50
Externe Betriebs- und Supportkosten	jährlich wiederkehrend	Fr. 721'400.00
Fortführende Investitionen	wiederkehrend ab 2. Betriebsjahr	Fr. 162'300.00
Summe inkl. Nutzungskosten Azure Office365 II (Lizenzen inkl. Advanced Security)		Fr. 3'633'337.50

Tabelle 26 Berechnung TCO

Ergänzung: Zwei Punkte werden die Berechnung der TCO beeinflussen:

- *Microsoft-Lizenzen: Microsoft hat das Lizenzierungsmodell für die Education-Lizenzen anfangs 2021 geändert. Die Berechnung erfolgt nicht mehr über das Vollzeitäquivalent sondern es müssen Einzellizenzen gelöst werden. Zu erwarten sind höhere Kosten im Bereich "Nutzungskosten Office365".*
- *Erweiterte Dienstleistungen: Zusätzlich zur Betreuung der Geräte wird die IZAB auch die Betreuung des Netzwerkes und der Peripheriegeräte übernehmen. Zu erwarten sind dadurch höhere Kosten im Bereich "Externe Betriebs- und Supportkosten".*

7. Anhang

7.1 Tabellenverzeichnis

Tabelle 1 Erläuterung der Zyklen	4
Tabelle 2 Stufe und Geräteausstattung	7
Tabelle 3 Berechnung Anzahl Endgeräte SuS	8
Tabelle 4 Berechnung Endgeräte Primarschule im Pool	9
Tabelle 5 Berechnung Anzahl Endgeräte LP	10
Tabelle 6 CYOD & BYOD.....	10
Tabelle 7 Berechnung Docking-Station / Aufbewahrung	11
Tabelle 8 Preissegment Windows Endgeräte	14
Tabelle 9 Minimalanforderungen Tablet Spezifikation.....	15
Tabelle 10 Tablet Zubehör Schutzhülle	15
Tabelle 11 Minimalanforderungen Convertible Spezifikation SuS.....	15
Tabelle 12 Convertible Zubehör für SuS Notebooktasche.....	15
Tabelle 13 Minimalanforderungen Convertible Spezifikation LP.....	16
Tabelle 14 Minimalanforderungen Notebook Spezifikation LP.....	16
Tabelle 15 Convertible und Notebook Zubehör für LP Dockingstation	16
Tabelle 16 Convertible und Notebook Zubehör für LP Notebooktasche.....	16
Tabelle 17 Inventarlisten	21
Tabelle 18 Lebenszyklen der bestehenden Endgeräte	21
Tabelle 19 Enterprise Mobility + Security Produkte.....	28
Tabelle 20 Grundlagen Entschädigungsmodell pro Endgerät.....	39
Tabelle 21 Berechnung Entschädigungsmodell pro Endgerät	39
Tabelle 22 Geräte-/Nutzertypen.....	41
Tabelle 23 Supportaufwand (2nd/3rd Level).....	42
Tabelle 24 Kurzbeschreibung TCO-Positionen.....	47
Tabelle 25 Anzahl Geräte.....	47
Tabelle 26 Berechnung TCO	48

7.2 Abbildungsverzeichnis

Abbildung 1 Personendaten und Datenschutz (DSG)	19
Abbildung 2 Schematischer Aufbau	24
Abbildung 3 Schnittstelle SIS - Azure AD.....	25
Abbildung 4 Office 365 Education	27
Abbildung 5 Übersicht MDM EM+S.....	28
Abbildung 6 Datenschutz und Datenablage	30
Abbildung 7 Bereitstellungsprozess Endgerät	31
Abbildung 8 Steuerung und Support	36
Abbildung 9 SLA / Support, Begriffsdefinitionen.....	43

8. Stichwortverzeichnis

Im Konzept verwendete Abkürzungen

BKS	Departement Bildung, Kultur und Sport im Kanton Aargau
BYOD	Bring Your Own Device; Bring dein eigenes Gerät
CYOD	Chose Your Own Device; Wähle dein eigenes Gerät
DEP	Apple Device Enrollment Program, steht für das offizielle Apple-Programm zur Geräteregistrierung
DOA	Dead-On-Arrival-Garantie, steht für defekt bei Ankunft
FTE	Full Time Equivalent, dt.: Vollzeitäquivalent (Abkürzung: VZÄ) oder Vollbeschäftigtenäquivalent ist eine Hilfsgrösse
IMAC	Ist ein Akronym aus dem Englischen. Es steht für Install, Move, Add und Change (dt.: Installieren, Verschieben, Hinzufügen und Verändern).
LAN	Local Area Network; Lokales kabelgebundenes Netzwerk
LP	Lehrperson
LCH	Dachverbands Lehrerinnen und Lehrer Schweiz (LCH)
MTTR	Mean Time To Repair, wird als die mittlere Reparaturzeit nach einem Ausfall eines Systems definiert.
OS	Operating System (Betriebssystem) oder die Oberstufenschule
PICTS	Pädagogischer ICT-Support
PS	Primarschule
RMA	Return Material Authorization, steht für Reparaturen/Garantiefälle
SaaS	Software as a Service ist ein Teilbereich des Cloud-Computing und die Software und die IT-Infrastruktur wird bei einem externen IT-Dienstleister betrieben und vom Kunden als Dienstleistung genutzt werden.
SAI	Schulen ans Internet, Angebot von Swisscom
SIS	Schulinformations- oder Schulverwaltungssystem (Datenbanken: LehrerOffice, Scholaris, usw.)
SLA	Service-Level-Agreement, bezeichnet einen Rahmenvertrag für Dienstleistungen und Support
SuS	Schülerinnen und Schüler
TICTS	Technischer ICT-Support
TCO	Total Cost of Ownership, steht für die Gesamtkostenberechnung und ist ein Abrechnungsverfahren, das helfen soll, alle anfallenden Kosten von Investitionsgütern, Betrieb und Support abzuschätzen.
VPP	Volume Purchase Program, steht für Volumenlizenzen über eine zentrale Lizenzierungsplattform für Apps
WLAN	Wireless Local Area Network; drahtloses lokales Netzwerk