Erziehungsdirektion des Kantons Bern

Direction de l'instruction publique du canton de Berne

Mittelschul- und Berufsbildungsamt

Office de l'enseignement secondaire du 2e degré et de la formation professionnelle

Kasernenstrasse 27
Postfach
3000 Bern 22
Telefon +41 31 633 87 00
Telefax +41 31 633 87 29
www.erz.be.ch
mba@erz.be.ch

Empfehlungen zur Einführung von BYOD

Schulen der Sekundarstufe II

Bearbeitungs-Datum	23.07.2018
Version	1b
Dokument Status	Freigegeben durch FA-ICT
Klassifizierung	Intern
Autor	Projektteam Empfehlungen zu BYOD und WLAN
Dateiname	Empfehlungen zur Einführung von BYOD V1b

Inhaltsverzeichnis

1 Zweck des Dokuments

1.1 Ausgangslage und Ziel

Das vorliegende Dokument leitet sich aus der ICT Strategie Schulen Sek II 2017 - 2021 des Mittelschul- und Berufsbildungsamts des Kantons Bern ab, die im Januar 2017 durch den Erziehungsdirektor freigegeben worden ist.

Mit Blick auf die Schweizer Mittel- und Berufsbildungs-Schullandschaft lässt sich feststellen, dass in den meisten Kantonen Bring Your Own Device (BYOD)-Konzepte in Erarbeitung sind oder bereits existieren. Zudem finden sich diverse Schulen, die mitten in der BYOD-Einführung sind oder BYOD bereits «flächendeckend» eingeführt haben.

Das vorliegende Dokument versteht sich als Empfehlung für Schulen der Sekundarstufe II, die an einer Einführung von BYOD interessiert sind. Es wurde durch ein Kernteam, bestehend aus Vertretern der beiden Fachgruppen ICT Kanton Bern Mittelschulen und Berufsfachschulen erarbeitet und dem Fachausschuss ICT sowie den beiden Konferenzen KSG und KBB (bzw. an den Unterkonferenzen) konsultiert. Die erarbeiteten Empfehlungen sollten einerseits strategische Grundsätze vermitteln und andererseits mit einer grossen Anzahl von Praxistipps unterstützen.

Der wichtigste Praxistipp sei an dieser Stelle erwähnt: Angehende BYOD-Schulen sollen sich mit Schulen vernetzen – und zwar auf strategischer, pädagogischer wie auch technischer Ebene –, die bereits BYOD-Erfahrungen haben. Insbesondere für die BYOD-Akzeptanz der Lehrerschaft ist dieser Punkt von zentraler Bedeutung. Ebenso wichtig sind folgende Punkte[1]:

- Die Zusammenarbeit zwischen Lehrpersonen und Lernenden/Studenten steht weiterhin im Zentrum. Technische Hilfsmittel schmälern die Bedeutung der Lehrperson nicht.
- Der Lehrplan bleibt verbindlich.
- Inhalt vor Technik: Gemäss dem Motto «Use ICT to Learn» statt «Learn how to use ICT» stehen die Inhalte und nicht die Technik und ihre Handhabung im Vordergrund einer BYOD-Einführung. Voraussetzung ist selbstverständlich, dass die Lehrpersonen die entsprechende Software (und Hardware) beherrschen, mit welcher sie unterrichten.
- Alltagsintegration statt Einzelfeuerwerk: Das Gerät soll nicht als attraktive Abwechslung eingesetzt, sondern bei Bedarf in der täglichen Arbeit verwendet werden, bei der ein Mehrwert zu erwarten ist.

Der Fokus soll schwerpunktmässig auf die Integration der eigenen Geräte in den Schul- und Lebensalltag der Lernenden gerichtet sein.

Die vorliegende Empfehlung fokussiert sich im «System Schule» auf den Menschen, die Organisation und die Technik. Da die Technik für das reibungslose Funktionieren der Geräte der Lernenden im Schulnetz zentral ist, wird auf ebendiesen Bereich stärker fokussiert. Wie bei jedem Informatikvorhaben, muss man sich auch bei der Einführung von BYOD dem Thema Informationssicherheit und Datenschutz (ISDS) auseinandersetzen.

Für die Einführung von BYOD stehen keine zusätzlichen finanziellen Mittel zur Verfügung. Die Umsetzung der Empfehlungen muss im Rahmen der bewilligten Budgets der Schulen erfolgen.

[1] Bericht von Beat Döbeli Honegger über BYOD Projektschule Goldau (http://www.projektschule-goldau.ch)

Sämtliche technische Angaben in diesem Dokument werden regelmässig überprüft und gegebenenfalls aktualisiert. Die vorliegenden Empfehlungen bezieht sich auf den Einsatz von sowohl Open Source Software wie auch kommerzieller Software.

1.2 Verwendete Begriffe und Abkürzungen

BFS	Berufsfachschule(n)
Big Data	Technologien zur Sammlung und Auswertung von grossen und komplexen Datenmengen
BYOD	Bring Your Own Device
Cloud	Bezeichnet die Bereitstellung von IT-Infrastruktur wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet.
Data Owner	Der Dateneigentümer (englisch: data owner) ist für einen bestimmten Teil der Unternehmensdaten zuständig.
EDUBERN	ICT-Plattform der Erziehungsdirektion des Kantons Bern
eLearning	Elektronisch unterstütztes Lernen
ERZ	Erziehungsdirektion des Kantons Bern
IaaS	Infrastruktur als Service (englisch: Infrastructure as a Service)
ICT	Information and Communication Technology
ILIAS	Integriertes Lern-, Informations- und Arbeitskooperations-System; freie Software zum Betreiben einer Lernplattform
ISDS	Informationssicherheit und Datenschutz
KBB	Konferenz der Berufsfachschulen des Kantons Bern
KSG	Konferenz der Schulleitungen der Gymnasien des Kantons Bern
MAC-Adresse	Die Media-Access-Control-Adresse bezeichnet die Hardware-Adresse jedes einzelnen Netzwerkadapters, die als eindeutiger Identifikator des Geräts in einem Rechnernetz dient.
MBA	Mittelschul- und Berufsbildungsamt
MiS	Mittelschule(n)
on Prem	Bezeichnet die Bereitstellung von IT-Infrastruktur in den eigenen Räumlichkeiten, vor Ort oder lokal.
PDF	Portable Document Format - (trans)portables Dokumentenformat
Power over Ethernet	Bezeichnet ein Verfahren, mit dem netzwerkfähige Geräte über das Ethernet-Kabel mit Strom versorgt werden.
Site-Survey	Bezeichnet die Anforderungserhebung an Funk- und Clientgeräte durch eine spezialisierte Firma, damit die Access Points optimal platziert werden können.
SuS	Schülerinnen und Schüler
SW	Software
WLAN	Wireless Local Area Network (deutsch: drahtloses lokales Netzwerk)

2 Empfehlungen an die Schulleitungen und operative Führung der Schulen

2.1 Übersicht Empfehlungen

Fokusbereich Mensch	Fokusbereich Organisation	Fokusbereich Technik
• Schulung der Lehrpersonen • Schulung der Lernenden/SuS • Weiterbildung der Lehrpersonen	• Kommunikation/Geräteempfehlungen • Technischer Support • Pädagogischer ICT-Support • Regelung bei Schäden oder Diebstahl • Finanzierung der Endgeräte von Lehrpersonen • Kosten für Ausdrucke • Lehrmittel und SW-Lizenzen • Handhabung bei Prüfungen • ISDS	• Internetzugang der Schule • WLAN-Infrastruktur • Stromversorgung • Outputmanagement • Beamer/Screenanbindung • Clouddienste • Benutzerkonten und Passwortverwaltung • Benutzerauthentifizierung • Schutzmassnahmen für Endgeräte

2.2 Empfehlungen Fokusbereich Mensch

2.2.1 Schulung der Lehrpersonen

Die Schulleitungen sollen die Ausbildung der Lehrpersonen im Technischen (Anbindung Beamer, drucken, usw.) und im Didaktischen (Einsatz Medien im Unterricht) so früh wie möglich im BYOD Projekt angehen.

Eine geeignete Schulung und Dokumentation (z.B. Kurzanleitung max. eine A4 Seite) für den Einsatz von Peripheriegeräten ist für die Lehrpersonen angebracht. Die Didaktik und der Einsatz der Unterrichtsmedien sollen in den Fachschaften frühzeitig erarbeitet und ausgetauscht werden. Die Zusammenarbeit sollte intensiviert und die Inhalte in geeigneten, kollaborativen Gefässen abgelegt werden.

Alle Lehrpersonen sollten die angeordneten verbindlichen SW-Produkte inkl. Datenspeicherung und die damit verbundene Informationssicherheit und Datenschutz respektieren.

Die periodische Schulung sollte, wenn immer möglich, verbindlich sein. Diese kann z.B. im Rahmen eines Fachschaftstages angeboten werden.

2.2.2 Schulung der Lernenden/SuS

Die Schulung der Lernenden sollte durch die Lehrpersonen erfolgen: WLAN-Zugang, Anwendung der Programme, Datenspeicherung, Printing, Informationssicherheit und Datenschutz, ICT-Richtlinien zur Verwendung der Infrastruktur, usw.

2.2.3 Weiterbildung der Lehrpersonen

Die technischen, methodischen, didaktischen wie auch die Anwendungskompetenzen sollten kontinuierlich erweitert und aufgefrischt werden. Sehr gut geeignet sind schulinterne Kurse, oder schulübergreifende Angebote.

2.3 Empfehlungen Fokusbereich Organisation

Es wird empfohlen, bei der Einführung von BYOD mit wenigen Pilotklassen zu beginnen.

2.3.1 Kommunikation/Geräteempfehlungen zuhanden der Lernenden/SuS, Lehrbetriebe und Lehrpersonen

Betroffene Lehrpersonen, Lernende/SuS und Lehrbetriebe sollten so früh wie möglich (idealerweise ein Jahr vor Unterrichtsbeginn) über die Einführung von BYOD-Klassen informiert werden, damit sie sich entsprechend vorbereiten können. Dies ist vor allem für die Lehrpersonen von zentraler Bedeutung. Lernenden/SuS und Lehrbetrieben sollten ebenfalls möglichst früh die minimalen Geräteanforderungen mitgeteilt werden. Eine allfällige Übernahme von Kosten für die BYOD Geräte durch den Lehrbetrieb ist eine Angelegenheit zwischen dem Lernenden und dem Lehrbetrieb und wird idealerweise im Lehrvertrag geregelt. Die Arbeit an mehreren Klassen wird erleichtert, wenn die Schule einen Gerätetypen und ein Betriebssystem empfiehlt. Auf die besonderen Anforderungen einzelner Berufs- und Fachgruppen soll Rücksicht genommen werden.

Um den Support und das Handling zu erleichtern, wird empfohlen, dass die ganze Schule mit der gleichen Lern- und Austauschplattform arbeitet (z.B. Moodle, Google Classroom, Office 365). Die Reduktion auf wenige und einzelne Plattformen erhöht die Effizienz. Einheitliche E-Mail-Adressen der Lernenden/SuS erleichtern die Kommunikation zusätzlich.

Die Definition von gemeinsamen oder schulübergreifenden Kommunikationsrichtlinien wird ebenfalls empfohlen.

Schulinterne Richtlinien zum Umgang mit sozialen Netzwerken und zur Kommunikation über solche sollten definiert werden.

2.3.2 Technischer Support

Die Schule sollte den technischen Support vor dem Start der Pilotklassen klar definieren und allen Beteiligten kommunizieren. Es wird empfohlen, den technischen Support für die Lehrpersonen täglich bereits vor Unterrichtsbeginn zu gewährleisten. Ebenso sollte ein Mitarbeitender des technischen Supports erreichbar und dessen Telefonnummer allen bekannt sein. Aus Ressourcengründen wird empfohlen, für die Lernenden/SuS keinen (oder nur minimalsten, bspw. Login, Anbindung an WLAN) Support anzubieten und dies von Anfang an mitzuteilen.

Für BYOD sind verschiedene Szenarien denkbar. Jedes dieser Szenarien bringt verschiedene Vor- und Nachteile mit sich, welche im Vorfeld zwingend geklärt werden sollten. Die finanziellen Möglichkeiten spielen für den Entscheid des passenden Szenarios eine wichtige Rolle.

Szenario	Lehrpersonen	Lernende/SuS
Die Schule verwaltet keine Endgeräte mehr.	**Alle BYOD** (Präsentation/Drucken durch Schule verwaltet)	**Alle BYOD** Prüfungen/QV müssen so angepasst werden, dass sie mit den

		zur Verfügung stehenden technischen Lösungen durchgeführt werden können.
Die Schule verwaltet Endgeräte für Lehrpersonen.	**Keine BYOD** Verwaltete Geräte am Vorbereitungsarbeitsplatz, im Schulzimmer (Präsentation/Drucken durch Schule verwaltet)	**Alle oder teilweise BYOD** (Je nach Berufsgruppen/Abteilungen vereinbart) Ausnahme: Schulgeräte in Labors für Prüfungen/QV, Spezialanwendungen wie CAD, Automation, 3D-Anwendungen usw.
Die Schule verwaltet teilweise Endgeräte.	**Teilweise BYOD** Je nach Beschäftigungsgrad und Funktion sind durch die Schule verwaltete Geräte vorhanden.	

2.3.3 Pädagogischer ICT-Support

Die Schule sollte einen pädagogisch-didaktischen Support als Schnittstelle zwischen der Technik und den Lehrpersonen einrichten und mit Stellenprozenten entlasten. Die Lehrpersonen sollten bereits vor Beginn des Projekts auf den pädagogisch-didaktischen Support zurückgreifen können. Nebst der Schulung von Lehrpersonen im Umgang mit digitalen Medien (z.B. konkrete Lernszenarien), spielt der pädagogische ICT-Support bei der Beratung der Schulleitung (Strategie «Digitalisierung») und der ICT-Dienste im Rahmen der Beschaffung von Informatikmitteln eine wichtige Rolle.

2.3.4 Regelung bei Schäden oder Diebstahl an Geräten in Besitz von Lernenden/SuS

Die Gefahr von Beschädigungen an Geräten Dritter steigt, z.B. durch grosse Anzahl Geräte, herumliegende Kabel. Der Kanton haftet gemäss Art. 100 des Personalgesetzes (PG, BSG 153.01) für den Schaden, den die Mitarbeiterinnen und Mitarbeiter (inkl. nebenamtlich Tätige) in Ausübung ihrer amtlichen Tätigkeit Dritten widerrechtlich zufügen. Die Lehrpersonen müssen somit keine Haftpflichtversicherung abschliessen zur Deckung von Schäden, die sie am Gerät eines/einer Lernenden/SuS verursachen. Sind Schäden grobfahrlässig oder mit Absicht verursacht worden, kann der Kanton jedoch Regress auf die Lehrperson(en) nehmen. Die privaten Bildungsanbieter sorgen für den entsprechenden Versicherungsschutz.

Die Lernenden/SuS und deren Eltern sind für ihre eigene Haftpflichtversicherung verantwortlich. (Achtung: bei verschiedenen Versicherern besteht kein Versicherungsschutz für Schäden aus dem Verlust oder der Beschädigung von Daten und Programmen [Software]). Zusätzlich wird empfohlen, dass die Lernenden/SuS eine Diebstahlversicherung sowie eine Garantieverlängerung für ihre privaten Geräte abschliessen.

Fragen aus der Praxis bezüglich Haftung bei BYOD-Geräten von Lehrpersonen wurden durch den Rechtsdienst MBA im Anhang C beantwortet.

2.3.5 Finanzierung der Endgeräte von Lehrpersonen

Lehrpersonen an BYOD-Klassen sollten auf ein persönliches mobiles Endgerät zurückgreifen können. Es wird empfohlen, die Anschaffung und Finanzierung detailliert zu re-

geln: Entweder wird den Lehrpersonen ein Schulgerät zur Verfügung gestellt oder sie erhalten einen jährlichen Beitrag und beschaffen das Gerät selber. In beiden Fällen hängt es stark mit den Möglichkeiten des technischen Supports zusammen.

Nebst der Anschaffung der Endgeräte, muss geklärt werden, wer für die Beschaffung von Peripheriegeräten und Zubehör (z.B. Maus, Pen, Tasche, Adapter) zuständig ist.

Erhalten die Lehrpersonen einen jährlichen Beitrag an ein persönliches Endgerät, muss geregelt werden, was mit dem Gerät beim Austritt passiert (z.B. Löschen von Software, Rückzahlung eines Betrages).

Die Schule ist verantwortlich, dass jede Lehrperson (auch solche mit Kleinstpensen sowie Stellvertretende) während des Unterrichts jederzeit Zugang zu einem Computer hat. Dies kann entweder über einen Pool von mobilen Endgeräten sein (Schwierigkeit der Geräteverwaltung) oder über einen fest installierten Computer in jedem Unterrichtszimmer.

2.3.6 Kosten für Ausdrucke

Schulen die bereits BYOD im Einsatz haben, haben festgestellt, dass die Kosten für Ausdrucke zurückgehen und dass die Pauschalen/Verrechnung an die Lernenden/SuS entsprechend angepasst werden müssten.

2.3.7 Lehrmittel und SW-Lizenzen

Die Verantwortung über die Auswahl sollte den einzelnen Fachschaften übertragen werden. Innerhalb der Fachschaften ist ein einheitliches Lehrmittel empfehlenswert.

Falls das Lehrmittel auch als eLehrmittel erhältlich ist, wird dessen Einsatz empfohlen. Ist das Lehrmittel nur kombiniert (gedruckt und elektronisch) verfügbar, wird empfohlen, den Lernenden einzeln zu überlassen, mit welchem sie arbeiten. Sollte das Lehrmittel nur gedruckt vorliegen, kann mit der Einwilligung des Verlages (!) eine PDF-Version erstellt werden oder allenfalls ein Wechsel des Lehrmittels in Betracht gezogen werden. Allerdings ist das Lehrmittel allein kein Grund, nicht digital arbeiten zu können.

Die Lernenden/SuS sollten – soweit möglich – vor Beginn des Unterrichts darüber informiert werden, welche Lehrmittel in welcher Form an der Maturitäts- resp. Lehrabschlussprüfung zugelassen werden.

Eine korrekte Lizenzierung der eingesetzten SW-Produkte ist unverzichtbar. Die Schule sollte definieren, welche SW obligatorisch ist und wie sie finanziert wird (z.B. zusammen mit dem Materialgeld).

2.3.8 Handhabung bei Prüfungen

Idealerweise können die Lernenden/SuS zu Beginn der Ausbildung über die Art und Weise (analog oder elektronisch) der Prüfungs- resp. Qualifikationsverfahren informiert werden. Wo dies nicht abschliessend möglich ist, sollten die Lernenden/SuS auf beide Varianten vorbereitet werden. Es wird deshalb empfohlen, Prüfungen während des Semesters auf verschiedene Arten durchzuführen: elektronisch (z.B. über Socrative, Moodle, Microsoft Forms), analog oder beides. Wo während Prüfungen eine technische Überwachung nicht möglich ist, sollte sich die Lehrperson so im Zimmer positionieren, dass sie die Bildschirme im Blick hat (z.B. hinten im Raum).

2.3.9 Informationssicherheit und Datenschutz

Wie bei jedem Informatikvorhaben, muss man sich auch hier dem Thema Informationssicherheit und Datenschutz (ISDS) annehmen. Die Verantwortung für die Daten liegt bei der Schulleitung als Data Owner. Sie regelt und sensibilisiert den Umgang mit den Daten in der Schule. Dies bedingt aber im ersten Schritt eine Klassifizierung der Daten, damit im weiteren Verlauf eine Zuweisung zum Schutzbedarf der Informationen, die Ablage der Daten (on Prem oder Cloud) und den technischen Hilfsmitteln (z.B. Verschlüsselung,) möglich wird.

Idealerweise wird für die Struktur der Datenklassifizierung die Informationsschutzverordnung[2] genutzt, wobei sich für die Schulen lediglich die Abstufungen «vertraulich», «intern» und «öffentlich» eignen; entsprechend sind die Zugriffsberechtigungen zuzuweisen. Die Schulleitung überprüft in regelmässigen Abständen die vergebenen Zugriffsberechtigungen.

Dies alles wird in einem ISDS-Dokument festgehalten, welches detailliert regelt, wer welche Daten wo speichern darf/muss und wer für das Backup zuständig ist. Beachten Sie dazu unbedingt die kantonalen Vorgaben[3]. In jedem Fall ist die Schule auch für die entsprechende Infrastruktur verantwortlich (z.B. Cloud, Server, Abgabe verschlüsselter Festplatten). Viele Lehrpersonen haben in diesem Bereich Schulungsbedarf; in einer allfälligen Schulung sollte auch die Sensibilisierung zum Datenschutz zwingend enthalten sein.

Es wird zudem empfohlen, die Lernenden in einer zusätzlichen Nutzungsvereinbarung darauf hinzuweisen, welches ihre Rechte und Pflichten in Zusammenhang mit digitalen Medien während des Unterrichts sind. Auch die möglichen Konsequenzen bei Verstössen sollten in diesem Papier geregelt werden. Konkret sollte ein Lernender, eine Lernende wissen, auf welche Daten er/sie über WLAN innerhalb und ausserhalb der Schule Zugriff hat und wie er/sie damit umzugehen hat.

Sachdaten
(Dazu gehören auch korrekt anonymisierte Personendaten)
Diese bedürfen keines besonderen Schutzes, die Bearbeitung/Speicherung in der Cloud ist zulässig.

Personendaten
Angaben über eine bestimmte oder bestimmbare natürliche oder juristische Person. Beispiele aus der Schule: Personalien einer Lehrperson. Foto eines erkennbaren Schülers.

Besonders schützenswerte Personendaten
Angaben über

- die religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung sowie die Rassenzugehörigkeit;
- den persönlichen Geheimbereich, insbesondere den seelischen, geistigen oder körperlichen Zustand, Massnahmen der sozialen Hilfe oder fürsorgerischen Betreuung, Abwesenheitsgründe;
- polizeiliche Ermittlungen, Strafverfahren, Straftaten und die dafür verhängten Strafen oder Massnahmen.

[2] Vgl. Verordnung über den Schutz von Informationen des Bundes vom 4. Juli 2007 [Ref. 8)
[3] Vgl. Rechtliche Grundlagen der Datenschutzaufsichtsstelle des Kantons Bern [Ref. 7]

Beispiele aus der Schule: Noten eines Schülers. Aufsatz einer Schülerin, in welchem erwähnt wird, dass die Lehrerin, Frau Muster, krankheitsbedingt für eine längere Zeit ausfällt.

Auf BYOD-Geräten ist die lokale Bearbeitung/Speicherung von Personen- oder besonders schützenswerten Daten nicht erlaubt und entsprechend zu unterbinden. Es müssen besondere Vorkehrungen (z.B. Verschlüsselung der Harddisk) getroffen werden, weil der Grundschutz sonst nicht sichergestellt ist. Entsprechend müssen solche Daten auch in der Cloud spezifisch geschützt werden (z.B. Verschlüsselung mittels Microsoft Azure Rights Management).

2.4 Empfehlungen Fokusbereich Technik

2.4.1 Internetzugang der Schule

Ein leistungsfähiges Netzwerk (z.B. kantonaler Service BE-LAN) mit mindestens 1 Gbit/s Übertragungsgeschwindigkeit und eine stabile Internetanbindung (z.B. kantonaler Service BE-WAN) gehören zu den zentralen Bestandteilen einer schulischen IT-Basisinfrastruktur.

Der Internetanschluss der Schule muss für die Online-Arbeit genügend Bandbreite und eine hohe Verfügbarkeit haben. Der Bandbreitenbedarf hängt stark von der Art sowie der Anzahl Endgeräte und der Internetnutzung ab. Ein ungefährer Richtwert könnte ca. 2 Mbit/s pro Endgerät sein (Download).

Die künftig wohl wachsende Abhängigkeit vom Internet setzt voraus, dass bei einem Totalausfall die Schule eine Lösung anbieten kann wie damit umgegangen wird. Es wird empfohlen, dass die Schule für den Fall eines flächendeckenden Ausfalls des Internetzuganges einen Notfallplan erarbeitet.

Es wird zudem empfohlen, dass die Schule mithilfe eines Contentfilters den Zugriff auf bestimmte Inhalte im Internet unterbindet.

Als Basis für den konzeptionellen Aufbau (Zonenkonzept) des Netzwerkes innerhalb der Schule, sollte die kantonale Weisung über die Netzwerksicherheit (Network Security Policy[4]) berücksichtigt werden.

2.4.2 WLAN-Infrastruktur

Für die Planung und den Aufbau einer Wireless-LAN Infrastruktur (z.B. kantonaler Service BE-WLAN) für den Unterricht wird folgendes Vorgehen empfohlen:

Nutzer und Geräte definieren
Ein wichtiges Kriterium für die Planung ist die erwartete User Experience (welche Geräte, welche Applikationen, etc.). Um sie zu definieren, muss in einem ersten Schritt erfasst werden, welche Anwender-Typen es gibt (Schüler, Lehrpersonen, Verwaltung, Gäste). Dazu kommen häufig weitere Geräte mit drahtloser Anbindung, vom Netzwerkdrucker bis zur Überwachungskamera.

[4] Vgl. Network Security Policy (NSP) Kanton Bern [Ref. 4]

Es empfiehlt sich folgende SSIDs auf der Wireless-LAN Infrastruktur bereitzustellen:

Verwendungszweck	Netzwerk-Zonen[5]	Bsp. SSID-Name
Geräte der Schulverwaltung	**Restricted Access** (Zugriff auf BEWAN-Service wie z.B. Time, wwwin möglich)	*Schulname*_Verwaltung
Managed Schulgeräte im Unterricht	**Untrusted** (Zugriff auf Schulnetzwerk möglich, aber nicht auf BE-WAN-Services)	*Schulname*_School
BYOD-Geräte	**Isoliert** Zugriff auf Internet	*Schulname*_BYOD
Gäste	**Isoliert** Zugriff auf Internet	Guest

Anforderungen bestimmen
Im einem zweiten Schritt ist die Mindestperformance pro Nutzergruppe zu definieren. Sprich: Wie hoch muss die Datenübertragungsrate des Wireless-Netzes mindestens sein.

Transaktionsdichte ermitteln
Im nächsten Schritt sollte geklärt werden, wie viele Anwender im Abdeckungsbereich der verschiedenen Zugangspunkte erwartet werden. Multipliziert mit der geschätzten nötigen Bandbreite ergibt sich daraus die minimal nötige Transaktionsdichte.

Abdeckung festlegen
In der Planung muss ausserdem berücksichtigt werden, wo das WLAN verfügbar sein soll – nur in Schulzimmern und Lehrerzimmern oder benötigen Sie auch im Treppenhaus, im Fahrstuhl oder zwischen den Gebäuden einen Internetzugang? Es wird empfohlen, ein Site-Survey von einer spezialisierten Firma erstellen zu lassen, um die Menge und die idealen Montageorte für die Wireless AccessPoints herauszufinden.

Nötige Ressourcen erfassen
Als letzter Schritt in dieser Phase der Planung sollte erfasst werden, welche Ressourcen (z.B. Erweiterung der UGV und Strom, Installation der AccessPoints) für die Implementierung nötig sind. Neue WLAN-Technologien wie 802.11ac Wave 2, 802.3bz Ethernet-Schnittstellen oder die Integration von Bluetooth stellen neue Anforderungen, beispielsweise an Power over Ethernet (PoE). Empfohlen wird ein zentrales Management der AccessPoints aufzubauen.

Gesundheit
Über die langfristigen gesundheitlichen Auswirkungen der WLAN-Technologie liegen noch keine gesicherten wissenschaftlichen Erkenntnisse vor. Die Strahlenleistung von WLAN-AccessPoints sind jedoch um ein Mehrfaches geringer als die gesamte Strahlenbelastung von Mobiltelefonen der Lernenden/SuS einer Klasse.

[5] Vgl. Network Security Policy (NSP) Kanton Bern [Ref. 4]

Schutz Endgeräte
Für WLAN SSIDs, welche nur BYOD-Geräte bedienen, empfiehlt sich die Prüfung einer Client-Isolation zum Schutz (Zugriff) der Endgeräte untereinander.

2.4.3 Stromversorgung

Bei 1:1-Computing-Szenarien muss eine ausreichende Stromversorgung der Geräte sichergestellt werden. Die heutigen Schulzimmer verfügen gegenwärtig in der Regel über zu wenige Steckdosenzugänge.

Vor einer Einführung von BYOD-Klassen sollten sämtliche Schulräume bezüglich Stromversorgung überprüft werden. Es wird empfohlen, an den Seitenwänden 3-5 dedizierte 3er-Steckdosen bereitzustellen. Die Stromkreise für die BYOD-Geräte sollten idealerweise gesondert und genügend hoch abgesichert sein (Einschaltströme!). Auf keinen Fall sollten Steckerleisten kaskadiert werden.

Zusätzlich sollten in den Schulräumen eine ausreichende Anzahl an Steckerleisten zur Verfügung gestellt werden. Achtung vor Stolperfallen!

Es wird ausserdem empfohlen, im öffentlichen Bereich der Gebäude Steckdosen oder Stationen zum Aufladen von Geräten zur Verfügung zu stellen.

2.4.4 Outputmanagement (Drucken)

Das Drucken mit BYOD-Geräten via WLAN/Internet stellt eine spezielle Herausforderung dar und braucht in der Regel zusätzliche Systeme und Installationen. Spezielle Lösungen (z.B. PaperCut, EveryOnePrint, Printix) ermöglichen das Versenden von Druckjobs mit BYOD-Geräten.

Idealerweise können die Benutzenden anschliessend mittels einer Authorisierungs-Methode (z.B. Badge, PIN, NFC [Handy], Chip-Karte) an öffentlich zugänglichen Multifunktionsgeräten die persönlichen Druckjobs ausführen und abholen. (Das Vorgehen wird Follow-Me oder Secure-Printing genannt.) Nicht abgeholte Druckjobs werden bei Bedarf von den Systemen automatisch nach einer vordefinierten Zeit gelöscht.

Mit einer zusätzlichen, geräteunabhängigen Drucker Management- und Monitoring-Lösung (z.B. Equitrac, SafeCom, oder Output Manager) kann die netzwerkweite Dokumentenausgabe überwacht, gemessen und verwaltet werden. Zu diesem Zweck verfolgt die Software die Kopier- und Druckaktivitäten detailliert. Kosten können einfach und akkurat bestimmten Personen, Abteilungen oder Gruppen zugeordnet werden. Natürlich können auch Kontingente eingerichtet oder Einschränkungen bezüglich Farbdruck zentral vorgegeben werden.

2.4.5 Beamer/Screenanbindung

Grundsätzlich kann der Anschluss eines Beamers oder eines Monitors/Screens mittels Kabel oder Wireless erfolgen. Dabei wird empfohlen, folgende Punkte zu beachten:

- Kabelanschluss:
  - Adapter für die verschiedenen Anschlusstypen (z.B. VGA, HDMI, DVI) sollten entweder vorhanden sein oder mitgebracht werden.
  - Falls die Adapter zur Verfügung gestellt werden, sollten sie diebstahlsicher aufbewahrt werden können.
- Wireless Präsentationssystem:
  - Geeignete Systeme sollten evaluiert werden (z.B. Apple TV, WePresent, Miracast, Barco Clickshare, ViaGo, Microsoft Wireless Display Adapter).
  - Der Bandbreitenbedarf für Videowiedergabe sollte geklärt sein (vgl. Empfehlung WLAN-Infrastruktur).

- Allfällige Applikation für die Nutzenden sollte zur Verfügung stehen (z.B. auf Memorystick, in der Cloud).
- Verständliche und nachvollziehbare Anleitungen sollten vorhanden sein.
- Allfällige Mediensteuerung (z.B. Extron, Arvis) wird benötigt, wenn zwischen den verschiedenen Anzeigesystemen umgeschaltet werden muss. Wichtig dabei ist, die Auflösung der verschiedenen Anzeigesysteme aufeinander abzustimmen.

2.4.6 Clouddienste

Mittels Clouddiensten können Unterrichtsmaterialien relativ einfach orts- und zeitunabhängig zur Verfügung gestellt werden. Die Schule muss definieren, welche Clouddienste für welche Anwendungsbereiche zur Verfügung gestellt werden. Dabei ist wichtig, dass folgende Rahmenbedingungen definiert werden:

- Welche Dienste dürfen für welche Daten verwendet werden (vgl. Empfehlung Informationssicherheit und Datenschutz)?
- Sollen spezifische Anwendungen für die Nutzung der Clouddienste auf dem Endgerät bereitgestellt werden oder wird ausschliesslich mit dem Browser gearbeitet?

Hinsichtlich der Lern- und Austauschplattform stellt sich die Frage, ob ein Clouddienst (z.B. Office 365, Nanoo.tv, Educanet2) oder eine On-Prem-Lösung (z.B. Ilias, Moodle) eingesetzt wird. Für den Fall, dass ein Clouddienst eingesetzt wird, wird der Betrieb der Plattform durch den Provider sichergestellt. Es stellt sich allenfalls die Frage der Anbindung an das schulinterne Benutzerverzeichnis (vgl. Empfehlung zur Benutzerkonten und Passwortverwaltung). Bei einer On-Prem-Lösung muss die Schule den Betrieb der Plattform sicherstellen.

2.4.7 Benutzerkonten und Passwortverwaltung

Grundsätzlich sollte jede/r Lernende ein eigenes Benutzerkonto haben, welches verwaltet wird. Unpersönliche Benutzer/innen müssen wenn immer möglich vermieden werden. Idealerweise werden die Benutzerkonten mittels eines Verzeichnisdienstes (z.B. Active Directory von Microsoft) oder extern bewirtschaftet.

Bei der Erstellung der Initialpasswörter muss definiert werden, wie ein allfälliger Passwortwechsel vorgenommen werden kann. Es existieren folgende beiden Ansätze:

- Initialpasswort muss beim ersten Login geändert werden (→ Portal für Passwortänderung sollte zur Verfügung gestellt werden).
- Initialpasswort wird so komplex ausgestaltet (z.B. Gross-/Kleinschreibung, Ziffern, Zahlen, Sonderzeichen – mind. 3 Merkmale davon und Mindestlänge von 8 Zeichen), dass es nicht geändert werden muss. Bei dieser Variante ist allerdings zu beachten, dass bestimmte Zeichen auf bestimmten Endgeräten nicht einfach so eingegeben werden können (z.B. @ oder \ auf Mac-Geräten).

Damit sich Benutzende beim Wechsel des Initialpassworts beim ersten Login nicht mit dem persönlichen Account auf dem WLAN anmelden müssen, kann ein Gäste-WLAN eingesetzt werden.

Vorteilhaft in Zusammenhang mit dem Passwortwechsel ist, wenn den Lernenden ein sogenanntes Self-Service Passwortportal zur Verfügung steht. In diesem Portal können die Nutzenden eine private E-Mail-Adresse oder eine Mobiltelefon-Nummer hinterlegen, auf welche ein neues Passwort geschickt werden kann. So kann auch sichergestellt werden,

dass vergessene Passwörter ausserhalb der Betriebszeiten des ICT-Supports zurückgesetzt oder geändert werden können.

Mittels geeigneter Softwareprodukte kann sichergestellt werden, dass sich die Benutzenden mit nur einem Benutzernamen nur einmal am System anmelden müssen, um auf alle von der Schule zur Verfügung gestellten Dienste zugreifen zu können (→ Single-Sign-on). Dies kann z.B. mittels LDAP[6] oder dem Einsatz eines Identity Management Systems (z.B. Identity & Access Management von NetIQ) erreicht werden. Die notwendigen Anforderungen, um externe Dienste anbinden zu können, werden bei den entsprechenden Dienstanbietern definiert. In Zusammenhang mit dem Projekt FIDES (Föderation von Identifikationsdiensten) wird mittelfristig eine Standardisierung und Anonymisierung von Benutzerkonten angestrebt. Dieses Projekt wird zurzeit durch Educa spezifiziert.

2.4.8 Benutzerauthentifizierung

Gemäss Empfehlungen der «Digitalen Gesellschaft zum Betrieb von Public WLAN-Infrastrukturen»[7], welche sich auf die einschlägigen Gesetze und Verordnungen (BÜPF; SR 780.1; Art. 15 und VÜPF; SR 780.11, Art. 19) abstützt, ist eine eindeutige Identifikation des Nutzenden im öffentlichen WLAN einer Schule nicht notwendig. Es empfiehlt sich allerdings trotzdem, den Zugang zum öffentlichen WLAN mit geeigneten Mitteln zu kontrollieren. Unpersönliche Accounts sind dabei zu vermeiden. Dabei ist zu beachten, dass die Privatsphäre der Benutzenden zu respektieren ist. Sobald Personendaten zur Nutzung des WLAN erhoben werden, fällt der Anbieter des WLAN unter das Schweizerische Datenschutzgesetzt (DSG). Dies hat zur Folge, dass gegenüber der betroffenen Person eine Auskunftspflicht entsteht. Ausserdem müssen Daten, welche für die Teilnehmeridentifikation erhoben wurden (z.B. Handynummer, IP-Adressen, Namen), während sechs Monaten aufbewahrt werden (Vorratsdatenhaltung).

2.4.9 Schutzmassnahmen für Endgeräten

Beim Einsatz von BYOD-Geräten ist es unerlässlich, dass die Nutzenden darauf sensibilisiert werden, dass sie ihre Endgeräte mit einem funktionierenden Virenschutz und aktuellen Virensignaturen ausgerüstet haben. Zudem ist es wichtig, dass die jeweils empfohlenen Sicherheitsupdates auf dem Betriebssystem und Anwendungen zeitnah installiert werden. Es wird empfohlen, dass die Schule einen Leitfaden zuhanden der BYOD-User/innen für den Schutz von Endgeräten zur Verfügung stellt.

Mit geeigneten technischen Massnahmen (z.B. Routing, Firewall) ist sicherzustellen, dass die Nutzerinnen und Nutzer mit ihren BYOD-Geräten lediglich auf die von ihnen benötigten Dienste Zugriff gewährt wird. Werden die Dienste als Clouddienste angeboten, kann lediglich ein Internet-Zugang zur Verfügung gestellt werden. Falls Dienste auf internen Systemen angeboten werden, so bieten sich Virtualisierungs-Technologien (z.B. VMware Horizon, Microsoft HyperV) an, mit welchen die Zugriffe auf interne Ressourcen kontrolliert und gesteuert werden können.

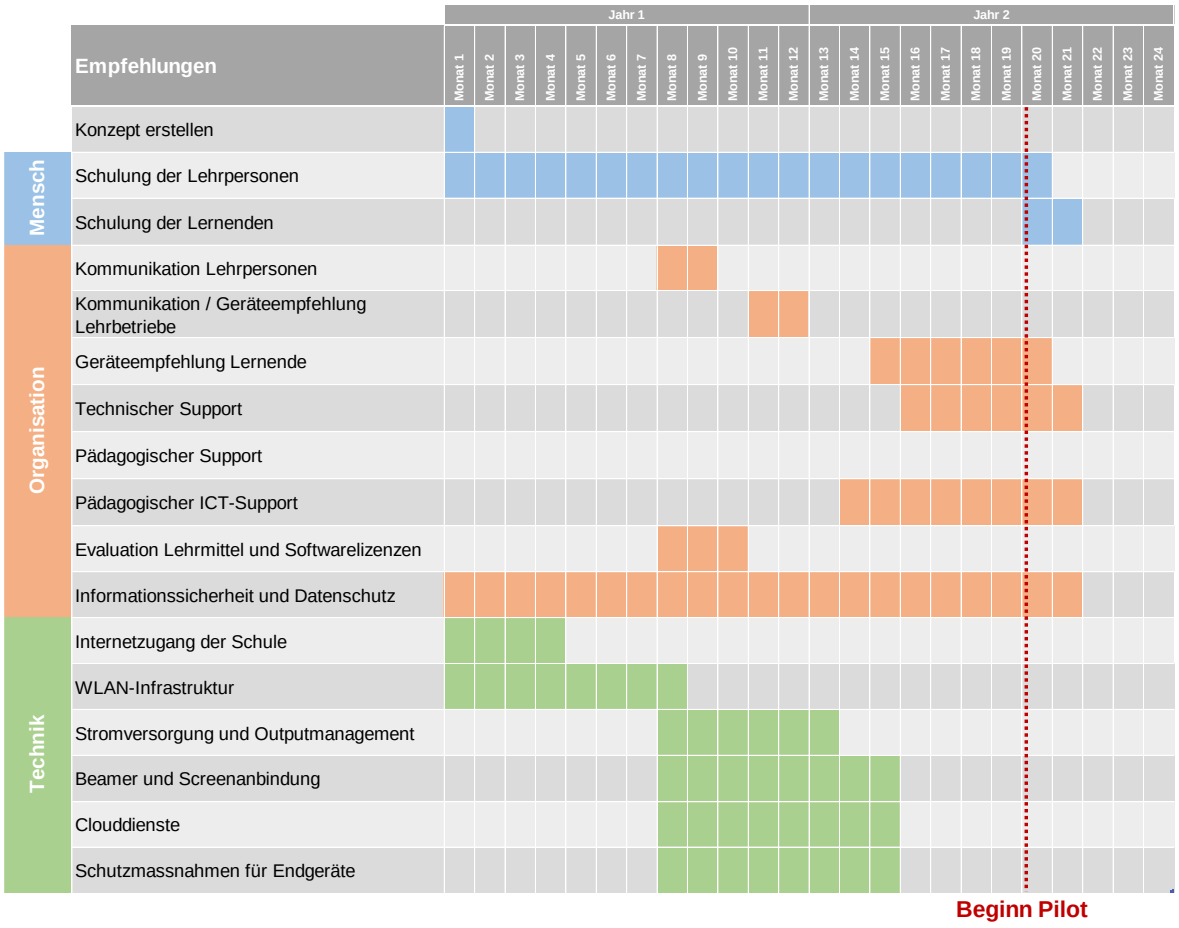
Für den Fall, dass mit Viren verseuchte Endgeräte am WLAN einer Schule angeschlossen sind, sollte sichergestellt werden können, dass diese Geräte identifiziert und von der Nutzung des WLANs ausgeschlossen (→ Deaktivierung des Benutzeraccounts oder Sperrung der MAC-Adresse des Geräts) werden können. Es empfiehlt sich, bei einer allfälligen

[6] https://de.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

[7] https://www.digitale-gesellschaft.ch/publicwlan/

Säuberung des Endgeräts den Lernenden Unterstützung durch eine ICT-Supportstelle anzubieten.

2.5 Zeitplan (Roadmap)



3 Kantonale Angebote zur Unterstützung der Schulen

Die IT-Services ERZ der Erziehungsdirektion des Kantons Bern unterstützen mit der Plattform EDUBERN[8] den Informationsmanagementbedarf der Schulen des Kantons Bern durch wirtschaftliche, harmonisierte und auf die Schulanforderungen zugeschnittenen Dienstleistungen und Services. Das Angebot umfasst Leistungen in sämtlichen Bereichen der ICT an Schulen: von Beratung über Betrieb und Support bis hin zu individuellen Lösungen.

Der Servicekatalog EDUBERN definiert die von der IT-Services ERZ angebotenen Serviceleistungen in den untenstehenden Kategorien:

[8] Weiterführende Informationen siehe EDUBERN Website (www.edubern.ch) oder EDUBERN Portal (http://portal.edubern.ch)

4 Weiterführende Informationen

Ref.	Thema	URL
[1]	21 Schritte – Ein Rahmenkonzept zur Planung und Umsetzung erfolgreicher 1:1 Computing Projekte der Microsoft Innovative Schools	https://blog.edu-ict.ch/wp-content/uploads/2016/01/4979.pdf
[2]	Beurteilung der digitalen Kompetenz Lehrender der europäischen Kommission	https://ec.europa.eu/jrc/sites/jrcsh/files/digcompedu_overview_-_german.pdf
[3]	BYOD-Guideline (2015) europäisches Netzwerk «European Schoolnet»	http://fcl.eun.org/documents/10180/624810/BYOD+Guideline+2015_DE.pdf/b83e3062-e1bc-478e-97f3-3e7b956d396f
[4]	Kantonale Weisung über die Netzwerksicherheit (Network Security Policy des Kantons Bern, NSP BE)	https://wwwin.kaio.fin.be.ch/intranet_kaio_fin/de/index/das_kaio/das_kaio/weisungen/1_3_informationssicherheit_und_datenschutz_isds.assetref/dam/documents/intranet_kaio_fin/das_kaio/de/Weisungen/1_3_011__Weisung_Netzwerksicherheit_NSP-BE.pdf
[5]	Leitfaden der Switch zur Datenklassifizierung beim Auslagern von Daten in die Cloud	https://www.switch.ch/de/stories/dataclassification/
[6]	Medien- und ICT-Konzept der Bildungsdirektion des Kantons Zürich	http://ict-guide.edu-ict.zh.ch/medien-und-ict-konzept
[7]	Rechtliche Grundlagen der Datenschutzaufsichtsstelle des Kantons Bern	http://www.jgk.be.ch/jgk/de/index/direktion/organisation/dsa/rechtliche_grundlagen.html
[8]	Verordnung über den Schutz von Informationen des Bundes vom 4. Juli 2007	https://www.admin.ch/opc/de/classified-compilation/20070574/201501010000/510.411.pdf

Anhang A: Geräteempfehlungen Lernende/SuS

Da die Geräte der Lernenden mindestens 3 bis 4 Jahre einwandfrei funktionieren sollten, sollte bei den Geräteempfehlungen nicht ein absolutes Minimum für störungsfreien Unterricht beschrieben werden. Den unterschiedlichen Anforderungen der einzelnen Berufe (Branchensoftware) ist unbedingt Rechnung zu tragen.

Bauform	Werden nebst Laptops auch Tablets erlaubt/empfohlen, macht in der Regel eine externe Tastatur Sinn.
Bildschirm	Die empfohlene Bildschirmdiagonale ist abhängig von den zu erwartenden Anwendungen. Werden grafikintensive Programme oder Arbeiten mit mehreren geöffneten Fenstern vorgesehen, sind grössere Bildschirme vorzuziehen (15 Zoll oder mehr). Dabei spielt allenfalls auch die Auflösung eine Rolle. In der Regel reichen Bildschirme ab 12 Zoll. Je nach Arbeitsweise und Anwendungen sollte auf die Vorteile eines Touch-Bildschirms hingewiesen werden.
Betriebssystem	Eine Empfehlung des Betriebssystems kann Sinn machen, wenn auf virtuelle Desktopumgebungen verzichtet wird. Damit wäre gewährleistet, dass alle Lernenden bei Erklärungen der Lehrperson ähnliche oder gleiche Ansichten hätten. Ebenfalls erleichtert es die Unterstützung durch die Lehrpersonen und/oder den IT-Support. Betriebssysteme absolut vorzuschreiben kann Schwierigkeiten hervorrufen, da viele Lernende bereits Geräte besitzen. Unbedingt abzuklären ist, was die eingesetzte und lokal installierte Software voraussetzt.
Software	Wird erwartet, dass die Lernenden bereits vor Lehrbeginn gewisse Software installieren (z.B. Virenschutz, PDF Reader), sollte dies mitgeteilt werden. Wird den Lernenden während der Lehrzeit Software zur Verfügung gestellt, sollte dies ebenfalls erwähnt werden, damit die Lernenden nicht unnötig Geld ausgeben (z.B. Office-Programme). Eine Information über die Konsequenzen bei Lehrabbruch oder Austritt ist sinnvoll.
Speicher	Der empfohlene Speicherplatz sollte für Dateien einer ganzen Lehrzeit ausreichend sein, damit nicht mit externen Datenträgern gearbeitet werden muss. Hierzu reichen in der Regel 128 GB. Ist vorgesehen mit Video- und/oder Bilddateien zu arbeiten, sollte dies zusätzlich berücksichtigt werden. SSD-Speicher sind vorzuziehen. Ein Hinweis auf allfällig eingesetzte Cloudspeicher und dessen Speicherplatz kann Sinn machen.
Arbeitsspeicher	Abhängig von der eingesetzten Software sollte eine Empfehlung zum Arbeitsspeicher gemacht werden. Für Standardprogramme reichen in der Regel 4 GB.
Prozessor	Abhängig von der eingesetzten Software sollte eine Empfehlung zum Prozessor gemacht werden. Für Standardprogramme reicht in der Regel i3 oder Vergleichbares.

Grafikkarte	Bei der vorgesehenen Verwendung von grafikintensiven Programmen sollte ein Hinweis auf die geforderte Leistung der Grafikkarte miteinbezogen werden.
Schnittstellen	Die Lernenden sollten in der Lage sein, ihr persönliches Gerät mit der Schulinfrastruktur zu verbinden (Beamer, Drucker, …). Je nachdem ist ein Hinweis auf die geforderten Schnittstellen, Kabel und entsprechenden Adapter notwendig. Zu berücksichtigen sind auch kabellose Möglichkeiten.
Zubehör	Je nach eingesetzter Software und vorgesehener Arbeitsweise bedingt der Einsatz von Computern Zubehör, das den Lernenden mitgeteilt werden kann. Es sind dies zum Beispiel Kopfhörer, Tastatur (bei Tablets), Maus, Adapter, Eingabestift. Den unterschiedlichen Arbeitsweisen der Lernenden sollte bei verbindlichen Vorgaben Rechnung getragen werden.
Anschaffung	Haben die Lernenden die Möglichkeit, über die Schule Geräte zu beziehen, kann es Sinn machen, sie an dieser Stelle darauf hinzuweisen. Eine ganz konkrete Auswahl weniger Geräte würde die Anschaffung erleichtern.
Weiteres	Weitere Hinweise zur Nutzung der Computer während des Unterrichts können den Lernenden bei den Geräteempfehlungen oder als separate Nutzungshinweise abgegeben werden. Im Wesentlichen sind dies Hinweise auf: • Versicherung und Diebstahl • Garantieverlängerung • PC-Support durch die Schule • erlaubte und verbotene Inhalte über das Schulnetz
Administratorenrechte	**Um Einstellungen vornehmen und Software installieren zu können, werden unbedingt lokale Administratorenrechte benötigt.**

Anhang B: Nutzungsvereinbarung Lernende/r oder SuS für elektronische Geräte im Unterricht

Die nachfolgende Regelung stammt aus der Praxis und sollte auf die Bedürfnisse der jeweiligen Schule angepasst werden.

1. **Verantwortung**
   Das Laptop ist persönliches Unterrichtsmaterial jedes/jeder Lernenden/SuS. Ihnen obliegt demzufolge die volle Verantwortung.
2. **Virenschutz und Updates**
   Die Lernenden/SuS sind verpflichtet, einen tauglichen und aktuellen Virenschutz zu installieren. Für die Updates sämtlicher Programme ist jede/r Lernende/SuS selber verantwortlich.
3. **Datenspeicherung**
   Für die Speicherung der Dateien gemäss Vorgabe der Schule, ist jede/r Lernende/SuS selber verantwortlich. Ein regelmässiges Backup auf einem externen Datenspeicher wird dringend empfohlen.
4. **Unterhalt**
   Mängel an Hard- und Software sind vor dem Unterricht zu beheben. Sollte dies nicht möglich sein, sind die Lehrpersonen spätestens am Vorabend davon in Kenntnis zu setzen.
5. **Vorbereitung**
   Als Lernende/r oder SuS sind Sie im Hinblick auf störungsfreien Unterricht verpflichtet, alle elektronischen Geräte mit vollgeladenem Akku zum Unterricht mitzubringen.
6. **Medienrecht**
   Das mit digitalen Medien zusammenhängende Recht (Urheberrecht, Recht am eigenen Bild, …) gilt insbesondere auch im Unterricht mit digitalen Medien. Zuwiderhandlungen werden gemäss Schulordnung, bei krassen Vergehen gemäss Strafrecht, geahndet.
7. **Nutzung**
   Die digitalen Medien sind während des Unterrichts nur zu den erlaubten Zeiten und für den erlaubten Zweck zu verwenden.
8. **Verbotene Inhalte**
   Es ist jederzeit verboten, pornografische, sexistische, rassistische, Gewalt verherrlichende und andere jugendgefährdende Inhalte aus dem Internet herunterzuladen, auf dem Schulareal zu zeigen oder auf dem Laptop gespeichert zu haben.
9. **Download und Upload**
   Es sind nur Up- und Downloads erlaubt, die in direktem Zusammenhang mit dem Unterricht stehen.
10. **Drucken**
    Gemäss schulspezifischen Vereinbarung sollte hier der Punkt Drucken geregelt werden.
11. **Schutz**
    Es ist Pflicht, den persönlichen Laptop mit einem Kennwort vor unerlaubten Zugriffen zu schützen. Besonders sensible Daten sollten mit einem zusätzlichen Passwort geschützt werden. Die Beschriftung des Geräts mit Vorname, Name, Klasse, … wird ebenfalls empfohlen.
12. **Ahndung von Vergehen**
    Bei Verdacht auf nicht zweckgebundenen Einsatz der digitalen Geräte hat die Lehrperson das Recht, sich vom Lernenden oder der/dem SuS die letzten Aktivitäten zeigen zu lassen. Die Lehrperson hat zudem die Möglichkeit, Vergehen gegen dieses Nutzungsreglement gemäss den Interventionsstufen der Schule gegen fehlbare Lernende vorzugehen.

13. Mitarbeit

Für einen reibungslosen und erfolgreichen Einsatz von digitalen Medien im Unterricht ist die ganze Klasse auf die Mitarbeit von allen Klassenmitgliedern angewiesen. Deshalb werden alle gebeten, bei Kenntnis von Mängeln oder Missständen zu reagieren und – falls nötig – die Lehrperson zu informieren.

14. Stromversorgung

Die Stromversorgung wird ausschliesslich für die schulische Nutzung elektronischer Geräte bereitgestellt.

Anhang C: Fragen/Antworten bezüglich Haftung BYOD-Geräten von Lehrpersonen

Die nachfolgenden Fragen bezüglich der Haftung bei privaten Geräten von Lehrpersonen stammen aus der Praxis und wurden durch den Rechtsdienst MBA wie folgt beantwortet:

Frage: **Wer haftet bei Diebstahl in der Schule bzw. wer zahlt bei Diebstahl?**

Antwort: Der Schaden ist der privaten Hausrat- oder Wertsachenversicherung zu melden. Sollte die private Versicherung nicht alle Kosten übernehmen, gilt Art. 54 PG:

Art. 54 PG Ersatz von Personen- oder Sachschaden
[1] Erleiden Mitarbeiterinnen und Mitarbeiter bei der Erfüllung ihrer Aufgaben einen Personen- oder Sachschaden, der weder von einem Dritten noch vom Arbeitgeber auf Grund einer anderen Regelung ersetzt wird, leistet der Arbeitgeber auf Gesuch hin Ersatz, sofern die Schädigung nicht ausschliesslich auf ihr Verschulden zurückzuführen ist. Der Ersatz kann bei Mitverschulden gekürzt werden.

Gesuche um Ersatz von Personen- oder Sachschaden gemäss Artikel 54 PG sind beim Personalamt auf dem Dienstweg einzureichen. Allfällige Ersatzleistungen werden direkt durch das Personalamt ausgerichtet (Art. 121 PV).

Frage: **Wer haftet bei Defekten in der Schule?**

Antwort: Hier ist zu unterscheiden zwischen Defekten, die durch die Lehrkraft selber verursacht werden oder die einfach so eintreten und Defekten, die von anderen Mitarbeitern verursacht werden:

<u>1. Defekt, durch die Lehrkraft selber verursacht oder einfach so eingetreten:</u>

Der Schaden ist der privaten Hausrat- oder Wertsachenversicherung zu melden. Sollte die private Versicherung nicht alle Kosten übernehmen, gilt Art. 54 PG:

Art. 54 PG Ersatz von Personen- oder Sachschaden
[1] Erleiden Mitarbeiterinnen und Mitarbeiter bei der Erfüllung ihrer Aufgaben einen Personen- oder Sachschaden, der weder von einem Dritten noch vom Arbeitgeber auf Grund einer anderen Regelung ersetzt wird, leistet der Arbeitgeber auf Gesuch hin Ersatz, sofern die Schädigung nicht ausschliesslich auf ihr Verschulden zurückzuführen ist. Der Ersatz kann bei Mitverschulden gekürzt werden.

Gesuche um Ersatz von Personen- oder Sachschaden gemäss Artikel 54 PG sind beim Personalamt auf dem Dienstweg einzureichen. Allfällige Ersatzleistungen werden direkt durch das Personalamt ausgerichtet (Art. 121 PV).

2. Defekt, der durch andere Mitarbeiter verursacht wird:

Zivilrechtliche Haftungsfrage (Art. 41 OR): Es ist Sache dieser zwei Lehrkräfte, die Streitigkeit zu klären. Der Schaden ist der privaten Versicherung zu melden. Sollte eine Lehrkraft keine solche private Versicherung haben oder die Versicherung sonst eine Haftung ablehnen, käme wiederum die Ersatzhaftung nach Art. 54 PG zum Zuge.