Kanton Bern
Canton de Berne

Bildungs- und Kulturdirektion
Amt für Kindergarten, Volksschule und Beratung
Regelschulen Deutsch

MERKBLATT APPLE SCHOOL MANAGER

Inhaltsverzeichnis

1 Einleitung

Dieses Merkblatt richtet sich an die verantwortlichen Stellen der Volksschulen, die das Produkt «Apple School Manager» als Dienstleistung nutzen wollen (Software as a Service). Es vermittelt ihnen einen groben Überblick über die Vorgehensweise, über nötige Vorabklärungen und über Massnahmen, die zu ergreifen sind, um «Apple School Manager» möglichst datenschutzkonform zu nutzen. Namentlich berücksichtigt werden Risiken, die bei der Nutzung der Cloud für Datenbearbeitungen auftreten, sowie Massnahmen, die zu treffen sind, wenn besonders schützenswerte Personendaten bearbeitet werden.

Hinweis:
Das Merkblatt ist eine Ergänzung zum Datenschutzlexikon des Kantons Bern.

2 Verantwortlichkeiten

Die Gemeinde trägt die alleinige Verantwortung für den Einsatz der angestrebten Infrastruktur mit Apple School Manager in ihrer Schule. Die kommunale Datenschutzaufsichtsstelle der Gemeinde prüft das Konzept und veranlasst unter Umständen Verbesserungen.
Die kommunale Datenschutzaufsichtsstelle kann sich mit datenschutzrechtlichen Fragen an die kantonale Datenschutzaufsichtsstelle wenden.

3 Vertragliche Ebene

Durch die Nutzung von Apple School Manager in der Volksschule entstehen für die verantwortlichen Behörden erhöhte Risiken im Bereich des Datenschutzes und der Informationssicherheit[1].

Ein wichtiges Instrument, um diese Risiken zu minimieren, ist der Side Letter zum bereits abgeschlossenen Apple-School-Manager-Vertrag der Schule. Apple garantiert darin die Anwendbarkeit von schweizerischem Recht und den Gerichtsstand Zürich.

Dieser Side Letter muss explizit durch die Schule und zusätzlich zum Apple-School-Manager-Vertrag eingefordert werden.

Trotz des Side Letters verbleiben im Zusammenhang mit der Bearbeitung von besonders schützenswerten Daten und der von Apple erhobenen Randdaten bestimmte Risiken. Diese können unter Umständen durch aufwendige technische Massnahmen beseitigt werden. Andere Risiken hingegen lassen sich nicht beseitigen oder allenfalls nur minimieren. Diese bleiben als sogenannte Restrisiken bestehen. Diese Restrisiken müssen ausgewiesen und der verantwortlichen Leitungsebene nachvollziehbar kommuniziert werden. Restrisiken, die die Leitungsebene als tragbar bewertet, können und müssen von dieser akzeptiert werden (Risikoakzeptanz).

Es gilt zu beachten, dass die vertraglichen Regelungen, insbesondere die Vertragsdauer, periodisch geprüft und allfällige Erneuerungen entsprechend geplant werden.

[1] Privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen» – privatim

4 Konzept

Bevor Apple School Manager implementiert und genutzt wird, ist ein Konzept zu erstellen, das die Inhalte der Kapitel 4.1 bis 6 regelt – insbesondere die beabsichtigte Bearbeitung von Daten und die vorgesehenen Schutzmassnahmen.[2]:

- Die Synchronisation von Personendaten mit der iCloud von Apple ist zu unterlassen (Vgl. Kapitel 3, Side Letter und Risiken). Ausnahme hierzu siehe 4.11.
- Nutzungsszenarien

  Welche Daten sollen für welchen Zweck auf welche Art und Weise bearbeitet werden?
- Klassifizierung der Daten

  Welchen Schutzbedarf weisen die eruierten Daten auf?
- Auswahl der geeigneten Dienste

  Mit welchen Apple-Diensten will die Schule welche Nutzungsszenarien umsetzen?
- Risiken erkennen und Schutzmassnahmen treffen

  Welchen Risiken ist die Personendatenbearbeitung ausgesetzt?
  Mit welchen angemessenen Massnahmen können diese Risiken beseitigt oder zumindest minimiert werden?
- Restrisiken ausweisen

  Bestimmte Risiken verbleiben bzw. können trotz Massnahmen nicht beseitigt werden. Diese Restrisiken müssen ausgewiesen und der verantwortlichen Leitungsebene nachvollziehbar kommuniziert werden. Restrisiken, die die Leitungsebene als tragbar bewertet, können und müssen von dieser akzeptiert werden (Risikoakzeptanz).

4.1 Nutzungsszenarien

Die Nutzungsszenarien für das «Ökosystem» von Apple stellen den Kern des Konzepts dar. Sie beschreiben die Bedürfnisse der Schule in Bezug auf die Digitalisierung. Sollten sich nach der Implementierung von Apple School Manager weitere Bedürfnisse zeigen, muss das Konzept ergänzt werden.
Die Nutzungsszenarien sollen mit allen beteiligten Personengruppen der Schule erarbeitet werden.

Folgende Punkte sollen in der Erarbeitung berücksichtigt werden:

- Nutzungsszenario im Rahmen der gesetzlichen Aufgabenerfüllung der Schule
  - Vorgängig muss die Zweckbindung geklärt werden
    - Beispiel für eine **legitime** Zweckbindung:
      «Die Lehrperson hält fest, was sie bei einer Schülerin oder einem Schüler beobachtet.»
    - Beispiel für eine **nicht** legitime Zweckbindung:
      «Alle Lehrpersonen einer Klasse möchten über die Lernstände der Schülerinnen und Schüler in sämtlichen Fachbereichen informiert sein.»
- Involvierte Personengruppen / Betroffene festhalten
- Die daraus resultierenden Produkte/Daten

Beispiel einer Zusammenstellung von Nutzungsszenarien

	Szenario	Betroffene	Produkte
1	Ergebnisse von Einzel- oder Gruppenarbeiten (kooperative Arbeitsformen) OHNE Personenbezug	Schülerinnen und Schüler, Lehrpersonen	Website, Dokument, Ton- und Videoaufnahmen

[2] Die Schulinformatik der PHBern unterstützt die Schulen in der Erarbeitung eines Cloudkonzepts.

2	Durchführung von Prüfungen/Tests	Schülerinnen und Schüler, Lehrpersonen	Dokumente, Tabellen (Auswertung)
3	Informationen an Erziehungsberechtigte der Klasse (Klassenlager, spezielle Anlässe…)	Schulleitung, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail
4	Kontaktdaten der Erziehungsberechtigten erfassen (Telefon, E-Mail) und der Klasse, den Lehrpersonen wie auch den Erziehungsberechtigten zugänglich machen. Nicht im Sinne einer Notfallliste mit Krankheitsbildern.	Schülerinnen und Schüler, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail
5	Dokumentieren des Mitarbeitergesprächs	Schulleitung, Lehrpersonen	Dokument
6	Erstellen von Förderplänen im Bereich Integration und einfache sonderpädagogische und unterstützende Massnahmen im Regelschulangebot (MR, ehemals IBEM).[3]	Lehrpersonen, Klassenlehrperson, Erziehungsberatung, Erziehungsberechtigte	Dokumente, Mail

4.2 Klassifizierung der Daten

Mithilfe eines Klassifizierungsprozesses ermitteln die Schulen, wie hoch der Schutzbedarf der Daten ist. Dabei werden folgende Ziele verfolgt:

- Grundlage für die Sensibilisierung bei den Nutzenden (Schulungen)
- Eruierung, welche Szenarien mittels einer Risikomatrix speziell untersucht werden müssen
- Eruierung des Schutzbedarfs von Daten ohne Personenbezug

Das Ampelsystem der PHBern[4] kann für die Kategorisierung von Daten eine Hilfestellung sein.

Die Produkte/Daten der einzelnen Szenarien werden analog der KRGV[5] wie folgt klassifiziert:

Schutzbedarf der Daten	**Datenklassifizierung des Kanton Berns**	**Beschreibung**
kein Schutzbedarf	Öffentlich	Diese Kategorie beschreibt Sachdaten wie beispielsweise Unterrichtsmaterialien ohne Personenbezug, anonymisierte Personendaten.
normaler Schutzbedarf	Intern	In diese Kategorie werden normale Personendaten erfasst. Beispiele: Vorname, Name, Emailadresse etc.
hoher Schutzbedarf	Vertraulich	Ein hoher Schutzbedarf besteht bei besonders schützenswerten Personendaten oder auch bei umfangreichen Sammlungen von normalen Personendaten wie auch Persönlichkeitsprofilen. Beispiele: Krankheiten, Straftaten, Notfall-Klassenliste mit weiteren Telefonnummern und evtl. Krankheiten, Klassen-Übersicht mit beurteilungsrelevanten Daten. Ebenfalls können auch Sachdaten unter dem Berufs- oder Amtsgeheimnis betroffen sein.

Beispiel einer Klassifizierung im Konzept:

	Szenario	Betroffene	Produkte	Klassifizierung
1	Ergebnisse von Einzel- oder Gruppenarbeiten (kooperative Arbeitsformen) OHNE Personenbezug	Schülerinnen und Schüler, Lehrpersonen	Website, Dokument,	Öffentlich

[3] vgl. die VMR, https://www.belex.sites.be.ch/data/432.271.1/de/
[4] https://kibs.ch/datenschutz/ampelsystem
[5] Verordnung vom 13. März 2013 über die Klassifizierung, die Veröffentlichung und die Archivierung von Dokumenten zu Regierungsratsgeschäften (Klassifizierungsverordnung, KRGV; BSG 152.17).

			Ton- und Videoaufnahmen	
2	Durchführung von Prüfungen/Tests inklusive Beurteilung	Schülerinnen und Schüler, Lehrpersonen	Dokumente, Tabellen (Auswertung)	Vertraulich
3	Informationen an Erziehungsberechtigte der Klasse (Klassenlager, spezielle Anlässe…)	Schulleitung, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail	Intern
4	Kontaktdaten der Erziehungsberechtigten erfassen (Telefon, E-Mail) und der Klasse, den Lehrpersonen wie auch den Erziehungsberechtigten zugängig machen. Nicht im Sinne einer Liste mit Krankheiten oder Allergien.	Schülerinnen und Schüler, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail	Intern
5	Liste mit Fotos und Namen der Schülerinnen und Schüler für die Lehrpersonen der Klasse	Schülerinnen und Schüler, Lehrpersonen	Dokument	Intern
6	Dokumentieren des Mitarbeitergesprächs	Schulleitung, Lehrpersonen	Dokument	Vertraulich
7	Erstellen von Förderplänen im Bereich Integration und einfache sonderpädagogische und unterstützende Massnahmen im Regelschulangebot (MR, ehemals IBEM).[6]	Lehrpersonen, Klassenlehrperson, Erziehungsberatung, Erziehungsberechtigte	Dokumente, Mail	Vertraulich
8	Die Nutzenden vergessen ihr Passwort	Alle Nutzerinnen und Nutzer	Daten	Intern

[6] vgl. die VMR, https://www.belex.sites.be.ch/data/432.271.1/de/

Einzelne Produkte in Zusammenspiel mit den Szenarien der Betroffenen können unterschiedlich klassifiziert werden.

Beispiel:

	Szenario	Betroffene	Produkte	Klassifizierung
5.a	Liste mit Fotos und Namen der Schülerinnen und Schüler für die Lehrpersonen der Klasse	Schülerinnen und Schüler, Lehrpersonen	Dokument	Intern
5.b	Liste mit Fotos und Namen der Schülerinnen und Schüler für die Lehrpersonen der Klasse (Integration einer Schülerin / eines Schülers mit visuell erkennbaren Beeinträchtigungen)	Schülerinnen und Schüler, Lehrpersonen	Dokument	Vertraulich

4.3 Auswahl der Dienste

Das «Ökosystem» von Apple bietet eine breite Palette von Diensten (Apps). Die Auswahl dieser Apps richtet sich nach den Bedürfnissen der Schule.
Es ist darauf zu achten, dass die Apps ihre Daten lokal speichern und dass nur Daten der Kategorie «*Öffentlich*» abgespeichert werden.
Apps von Drittanbietern inkl. der Speicherung von Daten (zum Beispiel Youtube) können nur ohne Personenbezug genutzt werden.

Weiter gilt zu beachten, dass Personendaten der Kategorie «*Vertraulich*» aufgrund der bestehenden Risiken nicht mit Apple-Diensten bearbeitet werden dürfen. Hierfür sind im Konzept andere Fachapplikationen zu berücksichtigen, die für die Bearbeitung vertraulicher Daten geeignet sind.

Beispiel einer Dienstauswahl im Konzept:

Datenklassifizierung	**gewählte App**
Öffentlich& intern	Deaktivierte Synchronisation der iCloud für Bearbeitung von internen Daten bei Pages, Numbers, Präsentationen, Garage Band, iMovie, Apple Mail, Kalender, Fotos, Notizen, Sprachmemos, Books, iTunes U, iTunes, Classroom oder bei Bearbeitung von internen Daten Verwendung von Microsoft 365 oder Google Workspace for Education mit educa Rahmenvertrag. Weitere Apps aus dem App-Store mit separatem Vertrag (Bsp. CH-Verlage)
vertraulich	Beurteilungsapplikation Kanton Bern[7] Lehreroffice, Tresorit, Protonmail, Klapp, Threema, Scolaris und andere (Vorabkontrolle durch Gemeinde nötig)

4.4 Risiken erkennen und Schutzmassnahmen treffen

Die Nutzungsszenarien und die daraus resultierenden Produkte/Daten werden unter Berücksichtigung der Klassifizierung auf realistische Risiken hin untersucht. Szenarien mit Produkten/Daten der Kategorie *«Öffentlich»* müssen nicht überprüft werden.

Bei der Kategorie *«Vertraulich»* sind erhöhte Anforderungen an den Schutz der Vertraulichkeit der Daten zu stellen und in der Risikoabwägung zu berücksichtigen. Die verantwortliche Behörde kann beispielsweise aufwendige technische Massnahmen mit einbeziehen (behördenseitige Verschlüsselung) und so eine Bearbeitung dieser Kategorie ermöglichen.

[7] https://www.beurteilung.apps.be.ch/beurteilung/SetLanguage.do

Die folgende Risikomatrix verdeutlicht, welche Risiken mit zusätzlichen Schutzmassnahmen minimiert werden müssen.
Die Ziffern der Achse «Eintrittswahrscheinlichkeit» werden mit den Ziffern «Auswirkung / Schadensausmass» multipliziert. Die Ergebnisse können in der Regel wie folgt gelesen werden:

- 1 und 2: Keine Massnahmen
- 3 – 6: Spezifischer Vertrag mit dem Anbieter der App/Apps und unter Umständen weiteres Konzept (zum Beispiel Microsoft, Google).
- 8 – 16: Wahl einer spezifischen Fachapplikation. Technische und schulorganisatorische Massnahmen können hier die Risiken bei Apple-Produkten nicht minimieren.

Eintrittswahrscheinlichkeit					
	4 sicher	4	8	12	16
	3 sehr wahrscheinlich	3	6	9	12
	2 wahrscheinlich	2	4	6	8
	1 unwahrschienlich	1	2	3	4
		1 unwesentlich	**2 geringfügig**	**3 kritisch**	**4 katastrophal**
	Auswirkung / Schadensausmass				

Beispiele von häufig eintretenden Risiken mit verschiedenen Schutzmassnahmen:

	Szenario/Risiko	Schadens-ausmass	Eintrittswahrscheinlichkeit	Risiko	Massnahmen
2.a	Durchführung von Produkten/Lernkontrollen inklusive Beurteilung (Prädikat/Benotung). Die Prüfungsresultate werden in der Schule publik.	2	3	6	Nur möglich in Kombination mit Microsoft (zu beachten Merkblatt M365). oder Die Lehrpersonen werden dahingehend geschult, dass sie die einzelne Beurteilung nicht in denselben Dokumenten vermerken, sondern diese in der entsprechenden Fachapplikation dokumentieren.
2.b	Dokumentation prognostische Beurteilungen/Einschätzungen. Würden solche Beurteilungen bekannt, könnte das den Betroffenen nachhaltig schaden, zum Beispiel im Zusammenhang mit der Berufswahl.	3	3	9	Nur möglich in Kombination mit Microsoft (zu beachten Merkblatt M365). oder Das Konzept der Schule sieht vor, dass diese vertraulichen Daten nur in der spezifischen Fachapplikation bearbeitet werden dürfen. Die Sensibilisierung/Schulung hierzu ist in [(Referenzen anfügen] ausgewiesen.
7.a	Förderpläne im Bereich Integration und einfache sonderpädagogische und unterstützende Massnahmen (MR, ehemals IBEM) werden erstellt und in Onedrive gespeichert. Administratoren von Apple können auf diese Daten zugreifen. Behördenzugriffe seitens der USA (Cloudact) sind aufgrund	3	4	12	Nur möglich in Kombination mit Microsoft. oder Förderpläne müssen mit einer lokalen Textverarbeitung erstellt und in Fachapplikationen mit entsprechender Sicherheit abgelegt werden.

	von fehlenden Kontrollmöglichkeiten nicht überprüfbar.				
7.b	Diese Förderpläne werden per E-Mail der Schulleitung oder auch den Erziehungsberechtigten zugestellt. Die Gefahr einer fälschlich eingegebenen E-Mailadresse oder bei der Verwendung von Verteilerlisten ist gross. Der Schaden für die betroffene Person kann unter Umständen kritisch sein (Mobbing, Cybermobbing)	3	4	12	Entweder: Mailinhalte und Anhänge an externe Mailadressen werden verschlüsselt. Das Passwort wird über einen zweiten Kanal übermittelt. Zusätzlich wird eine digitale Signatur eingesetzt (S/MIME). Oder: Für die Übermittlung dieser Inhalte per Mail wird ein separater Maildienst mit zusätzlicher Verschlüsselung eingesetzt. Beispiel: Protonmail. Dieser Maildienst wird mit einer Zwei-Faktor Authentifizierung betrieben. Oder: Dateien werden nur als Link auf einem dritten, sicheren Server mittels separatem Passwort freigegeben. Beispiel: Proton Drive oder Tresorit / Tresorit Send

4.5 Restrisiken ausweisen

Auch wenn die aufgeführten Massnahmen (Kombination von Apple Schoolmanager mit Microsoft 365 oder anderen Fachapplikationen) umgesetzt werden, verbleiben unter Umständen immer noch Risiken, die nicht auf ein tragbares Mass minimiert werden können (Restrisiken). Dies ist beispielsweise der Fall, wenn eine Schule oder Gemeinde entgegen der Empfehlung von *Kapitel 4.10 «Erfassen der Nutzerinnen und Nutzer»*, Vornamen und Nachnamen innerhalb des Apple-Schoolmanagers führt.

Zurzeit sind die meisten Restrisiken in fehlenden Kontrollmechanismen auszumachen. Diese Restrisiken müssen ausgewiesen, der verantwortlichen Leitungsebene nachvollziehbar kommuniziert und von dieser akzeptiert werden (Risikoakzeptanz).

Auch wenn die aufgeführten Massnahmen umgesetzt werden, können Risiken verbleiben (Restrisiken).
Zurzeit sind die meisten Restrisiken in fehlenden Kontrollmechanismen auszumachen.
Diese Restrisiken müssen ausgewiesen und der verantwortlichen Leitungsebene nachvollziehbar kommuniziert werden. Restrisiken, die die Leitungsebene als tragbar bewertet, können und müssen von dieser akzeptiert werden (Risikoakzeptanz).

<u>Beispiele</u>
Vertragsgebundene Restrisiken:

- Fehlende Überprüfbarkeit der Zugriffe auf die Daten durch Apple bzw. Subunternehmen von Apple.
- Fehlende Überprüfbarkeit der Zugriffe durch amerikanische Sicherheitsbehörden (Cloud Act).
- Die verantwortliche Behörde kann nicht überprüfen, ob Personendaten, die für eine Zwei-Faktor-Authentifizierung verwendet werden (Name, Vorname, geschäftliche Mail, unter Umständen private Mobile-Nummer) auch wirklich nach der vertraglich festgelegten Dauer der Speicherung unwiderruflich gelöscht werden.
- Die verantwortliche Behörde kann die Zusammenarbeit von Apple mit dem Side Letter von Apple nicht ausschliessen.
- Erfassung der Nutzenden mit Vor- und Nachnamen. Diese Personendaten bergen das Risiko des Profilings.
- Einseitige Vertragsanpassungen durch Apple.

4.6 Verschlüsselung

Bei der Nutzung von Apple School Manager ist standardmässig der Transportweg (TLS) und die Verschlüsselung der ruhenden Daten implementiert. Apple verfügt jedoch über den Schlüssel. Somit kann ein Supportmitarbeiter von Apple Einsicht in die Daten erhalten.
Der Apple Schoolmanager bildet die Grundlage für Apple-Dienste und Apple-Apps im Bildungsbereich; somit muss ihm besondere Aufmerksamkeit geschenkt werden.
Risiken können mit keinen technischen Massnahmen auf Seiten Apple Schoolmanager reduziert werden. Ebenfalls nicht ausgeschlossen ist, dass US-Behörden via Cloud Act Zugriff auf gespeicherte Daten haben können.

Auf dem Markt sind Lösungen für Datenspeicherung oder für E-Mail mit den stärksten Sicherheitstechnologien zu erhalten. Diese lassen sich via Apps gut in eine iOS-Umgebung integrieren. Wichtig ist es, abzuklären, ob vertraglich der Gerichtsstand Schweiz und das anwendbare Schweizer Recht sowie ein Serverstandort in der Schweiz oder in der EU vereinbart werden kann. Beispiele sind unter 4.3 «Auswahl der Dienste» zu finden.

4.7 Protokollierung

Der Apple School Manager führt ein Protokoll aller durchgeführten Aktivitäten. Es können die Einträge der letzten 30 Tage angezeigt werden. Danach werden die Daten von allen Apple-Servern gelöscht. Der Side Letter (Vgl. Kapitel 3) bietet diesbezüglich kaum Kontrollmöglichkeiten.

Eine Protokollierung oder «Loggen» ist für die Funktionstüchtigkeit eines Systems wichtig. Die Daten dürfen aber nur unter bestimmten Voraussetzungen ausgewertet werden (vgl. kantonale Randdatenverordnung RDV[8]):

- Bei technischen Problemen
- Bei Missbrauchsverdacht:
    - Eine hinreichende schriftliche Begründung des konkreten Missbrauchsverdachts
    - Einen erwiesenen Missbrauch
    - Eine schriftliche Information der betroffenen Person

Da die automatisierte Übermittlung von Daten an Apple nicht unterbunden werden kann, sind diese Probleme bei den Restrisiken zu vermerken (siehe 4.5).

4.8 Authentifizierung und Passwörter

Für Administratorinnen und Administratoren ist eine Zwei-Faktor-Authentifizierung notwendig. Diese kann Im Apple School Manager aktiviert werden und ist kostenlos.
Für Lehrpersonen wird die Zwei-Faktoren-Authentifizierung empfohlen. Der Verzicht auf eine Zwei-Faktoren-Authentifizierung (Anmeldung mit einem einzigen Single-Faktor) birgt ein hohes Risiko, da damit eine unrechtmässige Übernahme des Kontos durch eine andere Person ermöglicht wird.

Der Apple School Manager bietet grundsätzlich drei Arten der Authentifizierung:

- Verwendung der iCloud-Authentifizierung
- Synchronisation des Passworts mit einem Azure Active Directory

[8] https://www.belex.sites.be.ch/frontend/versions/1781/art8?locale=de

- Verwendung eines internen Authentifizierungsdienstes (beispielsweise Active Directory Federation Service) über die SAML-Schnittstelle

Die Art der Authentifizierung ist im Rahmen einer Risikoanalyse zu bestimmen. Dabei sind der Zweck und der Umfang der Datenbearbeitung sowie die Art der bearbeiteten Daten zu berücksichtigen.

4.9 Rollen- und Berechtigungen

Die erteilten Rollen- und Berechtigungen sind jährlich zu prüfen. Jede Person darf nur auf diejenigen Daten zugreifen können, die sie auch tatsächlich benötigt.

4.10 Erfassen der Nutzerinnen und Nutzer

Falls entgegen der Empfehlungen gleichwohl personalisierte Clouddienste genutzt werden, wird auf folgendes hingewiesen:
Apple bearbeitet nicht nur die innerhalb der Cloud-Dienste übermittelten Personendaten (also insbesondere Inhaltsdaten), sondern auch von den Nutzerinnen und Nutzer selbst bzw. von ihren Diensten generierte Daten über die Nutzerinnen und Nutzer (zum Beispiel Rand-, Telemetrie- oder Protokollierungsdaten). Diese zusätzlichen Personendaten sind mit der gleichen Sorgfalt zu behandeln wie die Daten, die zur eigentlichen Aufgabenerfüllung bearbeitet werden.

Folglich ist auch bei der Erfassung der Nutzerinnen und Nutzer darauf zu achten, dass nur die nötigsten Angaben erfasst werden (Datensparsamkeit).

Werden Nutzerinnen und Nutzer im Apple School Manager erfasst, sollen diese pseudonymisiert werden (Bsp. Vorname.ErsterBuchstabedesNachnamens@schulexyz.ch).
Viele Gemeinden haben bereits Software im Einsatz, die als Identitätsprovider (IdP) genutzt werden können. Beispiele:

- Evento
- iCampus
- Software der Einwohnerkontrolle

Diese IdP bieten die Möglichkeit eines Exports der Datenbank mit einer Identifikator-Nummer, die sich für eine Pseudonymisierung nutzen lässt.

4.11 Synchronisation von Nutzerdaten

Eine Synchronisation der Nutzerdaten mit der iCloud von Apple ist nur unter Berücksichtigung von Kapitel 4.10 möglich.

4.12 Löschen

Das Löschen der Daten kann analog physischer Daten betrachtet werden. Es gelten die Aufbewahrungspflichten des Kantons Bern. Daten, die nicht mehr benötigt werden, müssen gelöscht werden. Die Nutzerinnen und Nutzer sollen die Möglichkeit erhalten, ihre Daten vor der Löschung auf ein anderes Speichermedium zu transferieren.

Die Löschung der Protokolldaten erfolgt automatisiert.

4.13 Datensicherung und Notfallplanung

Die Anforderungen in Bezug auf die Verfügbarkeit von Apps sind zu definieren. Bei Bedarf sind entsprechende Massnahmen zur Datensicherung und Notfallplanung zu implementieren.

4.14 Diagnosedaten

Wird Hardware von Apple eingesetzt, werden möglicherweise Daten an Apple übermittelt. Da die Administratorinnen und Administratoren keine Möglichkeit haben, Massnahmen betreffend Diagnosedaten zu treffen, bleibt nur, das Restrisiko auszuweisen.

5 Informationen der betroffenen Personen

Nutzerinnen und Nutzer der Schule sind über den geplanten Einsatz von Apple-Hardware in Kombination mit dem Apple School Manager im Vorfeld zu informieren. Dabei sind die wichtigsten Risiken und die getroffenen Schutzmassnahmen offenzulegen.

Die Nutzerinnen und Nutzer erhalten eine Zusammenstellung, wie die Apple-Hardware in Kombination mit dem Apple School Manager und weiterer Software in der Schule genutzt wird.

Die Schulinformatik der PHBern bietet einen für jede Schule konfigurierbaren Ampelflyer an[9].

Beispiel eines Ampelflyers:

5.1 Schulung und Sensibilisierung

Die Schulungen zur Infrastruktur sowie die Sensibilisierung in datenschutzrelevanten Anwendungsbereichen soll beginnen, sobald die Infrastruktur implementiert ist und genutzt wird.

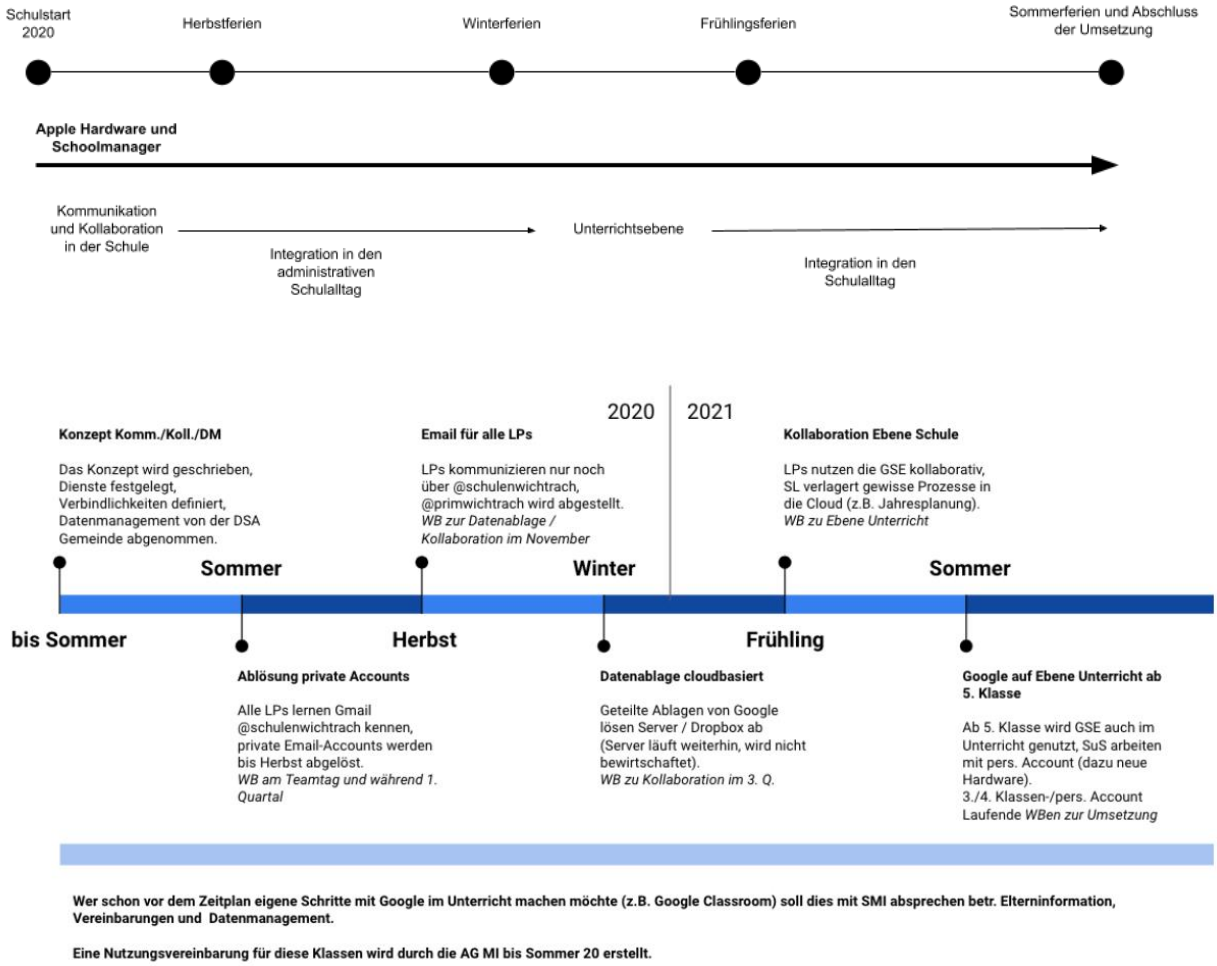
[9] www.kibs.ch

5.1.1 Lehrpersonen

Die Weisungen zum Umgang mit Daten in der Schule ergänzen die technischen Schutzmassnahmen (Vgl. 4.4 *Beispiele*).
Schulen sind mit starken Fluktuationen bei Lehrpersonen konfrontiert (Krankheiten und Stellvertretungen, Praxislehrpersonen). Hier gilt es sicherzustellen, dass neue Lehrpersonen unkompliziert und schnell die wichtigsten Informationen zur Nutzung der Schulhausinfrastruktur erhalten.

Die Erfahrungen der Schulinformatik der PHBern haben gezeigt, dass eine kontinuierliche Weiterbildung der Lehrpersonen zur Infrastruktur (zum Beispiel durch die Spezialistinnen und Spezialisten Medien und Informatik, SMI) nachhaltiger ist als eine einmalige Schulung durch eine externe Firma. Zur Entlastung der SMI-Lehrperson können Schulen zentrale Abläufe oder auch Sensibilisierungsthemen in Form von Dokumenten oder Videos zur Verfügung stellen.

Beispiel einer Planung zur Einführung von Apple Hardware und Schoolmanager über 1 Jahr



5.1.2 Schülerinnen und Schüler

Die Schulung der Schülerinnen und Schüler kann im Konzept Medien und Informatik der Schule unter den Anwendungskompetenzen des Modullehrplans Medien und Informatik subsumiert werden.

6 Eltern

Eltern sollen über den geplanten Einsatz von Apple Hardware in Kombination mit dem Apple School Manager frühzeitig (vor der Implementierung) informiert werden.

6.1 Information der Eltern

Die Information der Eltern soll auf mehreren Kanälen erfolgen. Einerseits sollen alle Konzepte zur Infrastruktur und zu Medien und Informatik im Unterricht (Vgl. Empfehlungen[10]) transparent und frei zugänglich sein. Andererseits sollen die Eltern auch die Möglichkeit erhalten, Fragen zu stellen und Bedenken zu äussern.

6.1.1 Dokumente

- Konzept Medien und Informatik (Konzept aus Empfehlungen des Kantons Bern) [11]– Beispiele für dessen Inhalt:
    - Unterricht und Unterrichtsentwicklung
    - Personalentwicklung
    - Kollaboration und Kommunikation
    - Datenmanagement und Rechtliches
    - Technik und Finanzierung
- Konzept zur Cloud-Infrastruktur / Cloudkonzept (Konzept gefordert aus diesem Merkblatt)

6.1.2 Veranstaltung

Die Information der Eltern kann über mehrere Kanäle erfolgen. Einerseits sollen alle Konzepte zur Infrastruktur und zu Medien und Informatik im Unterricht transparent und frei zugänglich sein, andererseits sollen Eltern auch die Möglichkeit erhalten, Fragen zu stellen und Bedenken zu äussern. Eine Veranstaltung zur geplanten Einführung der Informatikinfrastruktur mit allen Beteiligten (Gemeinde, kommunale Datenschutzaufsichtsstelle, Schulleitung, SMI, Lehrpersonen, eventuell Firmen und/oder PHBern) kann sehr hilfreich sein.

6.1.3 Kenntnisnahme

Wurde der Apple School Manager gemäss diesem Merkblatt implementiert, kann davon ausgegangen werden, dass die Erziehungsberechtigten die Umsetzung zur Kenntnis genommen haben.

[10] https://www.lp-sl.bkd.be.ch/content/dam/lp-sl_bkd/dokumente/de/startseite/themen/medien-und-informatik/medien-informatik-empfehlungen-d.pdf
[11] Unterstützung bietet kibs.ch, Schulinformatik PHBern