Kanton Bern
Canton de Berne

Direction de l'instruction publique et de la culture
Office de l'école obligatoire et du conseil
Section de l’offre ordinaire de l’école obligatoire, partie francophone (Section francophone)

NOTICE RELATIVE À APPLE SCHOOL MANAGER

Table des matières

1 Introduction

La présente notice est destinée aux services responsables des établissements de la scolarité obligatoire souhaitant utiliser le produit « Apple School Manager » en tant que service (« *Software as a Service* »). Elle vise à fournir un panorama général de la procédure, des clarifications préliminaires requises et des mesures à prendre pour assurer une utilisation d'Apple School Manager aussi conforme que possible à la législation sur la protection des données. Elle tient notamment compte des risques liés au traitement de données sur le Cloud et énonce les mesures à prendre s'agissant du traitement de données personnelles particulièrement dignes de protection.

La présente notice complète le lexique du canton de Berne « Protection des données à l'école obligatoire ».

2 Responsabilités

Les communes sont seules responsables de l'utilisation de l'infrastructure requise pour Apple School Manager au sein de leurs établissements scolaires. Les autorités communales de surveillance de la protection des données étudient les stratégies ad hoc et, le cas échéant, définissent des améliorations. En cas de questions, elles peuvent s'adresser au Bureau cantonal pour la surveillance de la protection des données.

3 Niveau contractuel

Pour les autorités responsables, l'utilisation d'Apple School Manager à l'école obligatoire s'accompagne de risques accrus dans les domaines de la protection des données et de la sécurité de l'information[1].

La lettre bilatérale (side letter) accompagnant le contrat Apple School Manager conclu avec l'école constitue un instrument important pour réduire ces risques autant que possible. Dans celle-ci, Apple garantit l'application du droit suisse et reconnaît Zurich comme for juridique.

L'école doit explicitement demander cette lettre bilatérale en complément du contrat Apple-School-Manager.

Malgré cette lettre bilatérale, certains risques demeurent concernant le traitement des données particulièrement dignes de protection et des données secondaires de communication collectées par Apple. Ces risques ne peuvent actuellement pas être réduits à un minimum acceptable, même au moyen de mesures techniques complexes. Tous les risques doivent être identifiés et présentés de façon compréhensible à l'échelon de direction compétent pour approbation (acceptation du risque).

Il convient de noter que les dispositions contractuelles, en particulier la durée du contrat, sont périodiquement examinées et, le cas échéant, les renouvellements sont planifiés en conséquence.

[1] Cf. nouvelle version révisée de l'aide-mémoire « Risques et mesures spécifiques au cloud » de privatim.

4 Stratégie

Avant d'introduire et d'utiliser Apple School Manager, il y a lieu d'élaborer une stratégie portant sur le contenu des points 4.1 à 6, notamment le traitement des données envisagé et les mesures de protection prévues à cet effet[2].

- Il convient d'éviter de synchroniser des données personnelles dans l'iCloud d'Apple (cf. point 3, lettre bilatérale et risques). Voir exceptions au point 4.11.
- Scénarios d'utilisation

  Quelles données peuvent être traitées, dans quel but et selon quelles modalités ?
- Classification des données

  Quel est le besoin de protection des données identifiées ?
- Choix des services appropriés

  Quels scénarios d'utilisation prévoit l'école et quels sont les services d'Apple nécessaires à cet effet ?
- Identification des risques et mise en œuvre de mesures de protection

  Quels risques comporte le traitement des données personnelles ?
  Quelles seraient les mesures indiquées pour éliminer ou tout au moins limiter ces risques ?
- Identification des risques résiduels

  Certains risques, dits résiduels, ne peuvent être éliminés par aucune mesure. Ils doivent être identifiés et communiqués clairement à l'échelon de direction compétent. La direction peut et doit accepter les risques qu'elle juge tolérables (acceptation du risque).

4.1 Scénarios d'utilisation

Les scénarios d'utilisation de l'« écosystème » d'Apple constituent le cœur du projet. Ils précisent les besoins de l'école dans le domaine de la numérisation. Si de nouveaux besoins sont identifiés postérieurement à l'introduction d'Apple School Manager, la stratégie devra être remaniée.
Les scénarios d'utilisation doivent être élaborés de concert avec toutes les parties prenantes au sein de l'école.

Lors de l'élaboration des scénarios, il convient de prendre en compte les points suivants :

- Scénarios d'utilisation dans le cadre de l'exécution des tâches légales de l'école
  - Il importe de vérifier au préalable l'affectation à des buts précis :
    - Exemple d'affectation à des buts **légitimes** :
      « L'enseignante ou l'enseignant consigne des observations concernant une ou un élève. »
    - Exemple d'affectation à des buts **non** légitimes :
      « L'ensemble des enseignantes et enseignants d'une classe souhaitent être informés du niveau d'apprentissage des élèves dans toutes les disciplines. »
- Groupes de personnes impliqués / concernés
- Produits et données obtenus

Exemples de scénarios d'utilisation

	Scénario	Personnes concernées	Produits

[2] Le Conseil en informatique scolaire de la PHBern aide les écoles à élaborer une stratégie d'utilisation du Cloud.

1	Résultats de travaux individuels ou de groupe (formes de travail collaboratives) SANS référence à des personnes	Élèves, membres du corps enseignant	Site Internet, documents, enregistrements audio et vidéo
2	Réalisation d'examens / de tests	Élèves, membres du corps enseignant	Documents, tableaux (évaluations)
3	Informations destinées aux parents d'élèves (par ex. camps et manifestations scolaires)	Directions d'école, membres du corps enseignant, personnes détenant l'autorité parentale	Documents, courriels
4	Saisie des coordonnées des parents (n° de téléphone, adresse électronique) et transmission de celles-ci aux élèves, aux membres du corps enseignant et aux personnes détenant l'autorité parentale(hors liste de numéros d'urgence avec informations concernant les maladies).	Élèves, membres du corps enseignant, personnes détenant l'autorité parentale	Documents, courriels
5	Documentation de l'entretien d'évaluation périodique (EEP)	Directions d'école, membres du corps enseignant	Documents
6	Élaboration de projets pédagogiques dans le domaine de l'intégration et des mesures de pédagogie spécialisée ordinaires et de mesures de soutien relevant de l'offre ordinaire de l'école obligatoire (MO, anciennement IMEP)[3]	Membres du corps enseignant, notamment maîtresse ou maître de classe, Service psychologique pour enfants et adolescents, personnes détenant l'autorité parentale	Documents, courriels

4.2 Classification des données

Les écoles se fondent sur une procédure de classification pour déterminer le besoin de protection nécessaire pour les données.
Les objectifs visés sont les suivants :

- Fournir une base pour la sensibilisation des utilisatrices et utilisateurs (formations)
- Évaluer quels scénarios en particulier doivent être examinés au moyen d'une matrice de risques
- Déterminer le besoin de protection pour les données sans référence à des personnes

Il peut être utile de se fonder sur le système de feux tricolores de la PHBern[4] pour établir la classification des données.

Par analogie avec l'ordonnance sur la classification, la publication et l'archivage des documents relatifs aux affaires du Conseil-exécutif (OCACE)[5], les produits et données correspondant aux divers scénarios sont classifiés comme suit ::

Besoin de protection	Classification dans le canton de berne	**Description**

[3] Cf. ordonnance régissant les mesures de pédagogie spécialisée ordinaires et les mesures de soutien relevant de l'offre ordinaire de l'école obligatoire (OMO ; RSB 432.271.1), www.belex.sites.be.ch/app/fr/texts_of_law/432.271.1
[4] https://kibs.ch/datenschutz/ampelsystem
[5] RSB 152.17.

Aucun besoin de protection	Public	Cette catégorie concerne les données factuelles, par ex. le matériel d'enseignement sans référence à des personnes ou les données personnelles anonymisées.
Besoin de protection normal	Interne	Cette catégorie recouvre les données personnelles ordinaires. Exemples : nom, prénom, adresse électronique, etc.
Besoin de protection élevé	Confidentiel	Les données personnelles particulièrement dignes de protection et les recueils volumineux de données personnelles ordinaires ou de profils de personnalité ont un besoin de protection élevé. Exemples : maladies, infractions pénales, liste en cas d'urgence dans la classe (numéros de téléphone supplémentaires et éventuellement informations concernant des maladies), vue d'ensemble de la classe avec données pertinentes pour l'évaluation. Il peut également s'agir de données factuelles soumises au secret professionnel ou de fonction.

Exemple de classifications dans la stratégie :

	Scénario	Personnes concernées	Produits	Classification
1	Résultats de travaux individuels ou de groupe (formes de travail collaboratives) SANS référence à des personnes	Élèves, membres du corps enseignant	Site Internet, documents, enregistrements audio et vidéo	Public
2	Réalisation d'examens / de tests, y c. évaluations	Élèves, membres du corps enseignant	Documents, tableaux (évaluation)	Confidentiel
3	Informations destinées aux personnes détenant l'autorité parentale (camps scolaires, manifestations spéciales, etc.)	Directions d'école, membres du corps enseignant, personnes détenant l'autorité parentale	Documents, courriels	Interne
4	Saisie des coordonnées des personnes détenant l'autorité parentale (n° de téléphone, adresse électronique) et transmission de celles-ci aux élèves, aux membres du corps enseignant et aux personnes détenant l'autorité parentale. Hors listes de maladies ou d'allergies.	Élèves, membres du corps enseignant, personnes détenant l'autorité parentale	Documents, courriels	Interne
5	Liste des élèves (noms et photos) destinée aux enseignantes et enseignants de la classe	Élèves, membres du corps enseignant	Documents	Interne
6	Documentation de l'EEP	Direction d'école, membres du corps enseignant	Documents	Confidentiel
7	Élaboration de projets pédagogiques dans le domaine de l'intégration ainsi que mesures de pédagogie spécialisée ordinaires et mesures de soutien relevant de l'offre ordinaire de l'école obligatoire (MO, anciennement IMEP)[6]	Membres du corps enseignant, notamment maîtresse ou maître de classe, Service psychologique pour enfants et	Documents, courriels	Confidentiel

[6] Cf. OMO.

		adolescents, personnes détenant l'autorité parentale		
8	Oubli du mot de passe	Ensemble des utilisatrices et utilisateurs	Données	Interne

Il est en outre possible de classifier différemment certains produits au sein d'un même scénario.

Exemple :

	Scénario	Personnes concernées	Produits	Classification
5.a	Liste des élèves (noms et photos) destinée aux enseignantes et enseignants de la classe	Élèves, membres du corps enseignant	Documents	Interne
5.b	Liste des élèves (noms et photos) destinée aux enseignantes et enseignants de la classe (intégration d'élèves présentant des handicaps visuellement indentifiables)	Élèves, membres du corps enseignant	Documents	Confidentiel

4.3 Choix des services appropriés

L'« écosystème » d'Apple offre une large palette de services (applications). Le choix de ces applications dépend des besoins de l'école.
Il convient de veiller à ce que les applications sauvegardent leurs données en local et que seules les données de la catégorie « public » soient sauvegardées.
Les applications de tiers, y compris la sauvegarde des données (p. ex. Youtube) ne peuvent être utilisées que sans référence à des personnes.

Il importe de préciser que, compte tenu des risques encourus, les données personnelles de la catégorie « confidentiel » ne doivent généralement pas être traitées dans le cadre des services d'Apple. Le cas échéant, il y a lieu d'inclure dans la stratégie d'autres applications spécialisées compatibles avec le traitement de données confidentielles.

Exemple de services retenus dans la stratégie :

Classification des données	**Application choisie**
Public et interne	Synchronisation désactivée de l'iCloud pour le traitement de données internes dans Pages, Numbers, Keynote, Garage Band, iMovie, Apple mail, Calendrier, Photos, Notes, Dictaphone, Livres, iTunes U, iTunes, Classroom ou, lors du traitement de données internes, utilisation de Microsoft 365 ou Google Workspace for Education avec le contrat-cadre Educa. Autres applications de l'App-Store avec contrat séparé (p. ex. maisons d'édition suisses)
Confidentiel	Application d'évaluation du canton de Berne[7] Lehreroffice, Tresorit, Protonmail, Klapp, Threema, Scolaris, etc. (nécessité d'un contrôle préalable par la commune)

[7] www.beurteilung.apps.be.ch

4.4 Identification des risques et mise en œuvre de mesures de protection

Les différents scénarios d'utilisation et les produits et données qui en résultent doivent être soumis à une évaluation réaliste des risques fondée sur la classification. Il n'est pas nécessaire de contrôler les scénarios comprenant des produits ou données appartenant à la catégorie « public ».

Pour la catégorie « confidentiel », il convient de fixer des exigences accrues concernant la protection de la confidentialité des données et de les intégrer dans l'évaluation des risques. L'autorité compétente peut ainsi inclure des mesures techniques complexes (cryptage par les autorités) pour permettre le traitement des données relevant de cette catégorie.

La matrice de risques ci-après présente les risques devant être limités par des mesures de protection supplémentaires.
Les chiffres de l'axe « Probabilité de survenue » doivent être multipliés par les chiffres de l'axe « Effet / étendue du dommage ». Les résultats se lisent généralement comme suit :

- 1 et 2 : aucune mesure nécessaire
- 3 à 6 : contrat spécifique avec le prestataire des applications et éventuellement stratégie complémentaire (p. ex. Microsoft, Google)
- 8 à 16 : choix d'une application spécialisée spécifique. La mise en œuvre de mesures techniques et organisationnelles au niveau de l'école ne peuvent pas limiter les risques liés aux produits Apple.

Probabilité de survenue	**4 certaine**	4	8	12	16
	3 très vraisemblable	3	6	9	12
	2 vraisemblable	2	4	6	8
	1 improbable	1	2	3	4
		1 négligeable	**2 minime**	**3 critique**	**4 catastrophique**
	Effet / étendue du dommage				

Exemples de risques fréquents et de mesures de protection possibles :

	Scénario/risque	Étendue du dommage	Probabilité de survenue	Risque	Mesures de protection
2.a	Produit : contrôles des connaissances, y c. évaluations (prédicat/notation) Les résultats sont divulgués dans l'école.	2	3	6	Seulement possible en combinaison avec Microsoft (voir *Notice Microsoft 365*). ou Les membres du corps enseignant sont formés à ne pas faire figurer certaines évaluations dans le même document, mais à les documenter dans l'application spécialisée prévue à cet effet.
2.b	Documentation d'évaluations/d'estimations pronostiques La divulgation de ces évaluations est susceptible de nuire durablement aux personnes concernées, notamment dans le cadre du choix professionnel.	3	3	9	Seulement possible en combinaison avec Microsoft (voir *Notice Microsoft 365*). ou La stratégie de l'école stipule que ces données confidentielles peuvent être traitées uniquement dans l'application spécialisée spécifique. La sensibilisation/formation dans ce domaine

					est indiquée dans le document « [Referenzen anfügen] ».
7.a	Élaboration de projets pédagogiques dans le domaine de l'intégration ainsi que mesures de pédagogie spécialisée et mesures de soutien (MO, anciennement IMEP), et sauvegarde dans OneDrive Les administratrices et administrateurs d'Apple peuvent avoir accès à ces données. Il n'existe aucune possibilité de contrôler si les autorités américaines consultent ces données (en vertu du *CLOUD Act*).	3	4	12	Seulement possible en combinaison avec Microsoft (voir *Notice Microsoft 365*). ou Les projets pédagogiques doivent être élaborés dans un système local de traitement de texte et sauvegardés dans des applications spécialisées sécurisées.
7.b	Les projets pédagogiques sont envoyés par courriel à la direction d'école ou aux personnes détenant l'autorité parentale. Le risque est élevé lors de la saisie d'une adresse électronique, et de l'utilisation de listes de distribution. Le dommage pour la personne concernée peut être considérable (harcèlement, cyberharcèlement).	3	4	12	1re possibilité : le contenu des courriels et les annexes envoyés à des adresses électroniques externes sont cryptés. Le mot de passe est transmis via un deuxième canal. Une signature numérique est utilisée (S/MIME). 2e possibilité : un service de messagerie distinct offrant un cryptage supplémentaire est utilisé pour transmettre les contenus. Exemple : Protonmail. Ce service de messagerie requiert une authentification à deux facteurs. 3e possibilité : les données sont communiquées uniquement sous forme de liens par le biais d'un troisième serveur sécurisé. Le mot de passe est envoyé séparément. Exemple : Proton Drive ou Tresorit / Tresorit Send

4.5 Identification des risques résiduels

Même si toutes les mesures énoncées sont mises en œuvre (combinaison d'Apple School Manager avec Microsoft 365 ou d'autres applications spécialisées), il reste certains risques qui ne peuvent pas être réduits dans des proportions tolérables (risques résiduels). C'est par exemple le cas lorsqu'une école ou une commune saisit des noms et prénoms dans Apple School Manager, contre les indications mentionnées au point 4.10 *Saisie des utilisatrices et utilisateurs*.

La mise en œuvre des mesures énoncées ne permet pas d'écarter tous les risques (risques résiduels). À l'heure actuelle, la plupart des risques résiduels résultent de l'absence de mécanismes de contrôle. Ils doivent être indiqués et communiqués clairement à l'échelon de direction compétent. La direction peut et doit accepter les risques qu'elle juge tolérables (acceptation du risque).

Exemples
Risques résiduels liés au contrat :

- Impossibilité de contrôler l'accès aux données par Apple ou des sous-traitants d'Apple
- Impossibilité de contrôler l'accès aux données par les autorités de sécurité américaines (en vertu du *CLOUD Act)*
- Impossibilité pour l'autorité compétente de contrôler que les données personnelles utilisées pour l'authentification à deux facteurs (nom, prénom, adresse électronique professionnelle et, dans certains cas, numéro de téléphone portable privé) sont bel et bien supprimées de manière irrévocable à l'expiration de la durée de conservation prévue dans le contrat
- Impossibilité pour l'autorité compétente d'exclure avec la lettre bilatérale la collaboration d'Apple avec des sous-traitants
- Saisie des noms et prénoms des utilisatrices et utilisateurs (risque de profilage)
- Modifications de contrat unilatérales par Apple.

4.6 Cryptage

Lors de l'utilisation d'Apple School Manager, la voie de transport (protocole TLS) et le cryptage des données au repos est mise en œuvre conformément aux normes applicables en la matière. Toutefois, Apple dispose de la clé de décryptage. Ainsi, une collaboratrice ou un collaborateur d'Apple peut accéder aux données.
Apple School Manager est la base des services et applications d'Apple dans le domaine de la formation. Aussi convient-il d'y conférer une attention toute particulière.
En ce qui concerne Apple School Manager, aucune mesure technique ne permet de réduire les risques. En outre, il n'est pas exclu que les autorités américaines, en vertu du *Cloud Act,* se procurent l'accès aux données sauvegardées.

Il existe sur le marché des solutions de sauvegarde des données ou de courriel dotées des technologies de sécurité les plus puissantes. Celles-ci sont facilement intégrables dans un environnement iOS, au moyen d'applications. Il est important de vérifier s'il est possible de convenir contractuellement du for juridique en Suisse, de l'application du droit suisse et du fait que les serveurs sont situés en Suisse ou au sein de l'UE. Des exemples sont présentés au point 4.3 *Choix des services appropriés*.

4.7 Procès-verbal

Apple School Manager tient un procès-verbal de toutes les activités réalisées. Les activités des 30 derniers jours peuvent être affichées. Au-delà de cette période, les données sont supprimées de tous les serveurs d'Apple. La lettre bilatérale (cf. point 3) n'offre à ce sujet que peu de possibilités de contrôle.

La tenue d'un procès-verbal est importante pour l'efficacité d'un système. Les données ne peuvent toutefois être exploitées que dans des conditions précises (cf. ordonnance cantonale sur les données secondaires de communication [ODSC][8]) :

- En cas de problème technique
- En cas d'utilisation abusive soupçonnée, si les conditions suivantes sont remplies :
    - le soupçon concret d'utilisation abusive est motivé par écrit de manière suffisante ou
    - l'utilisation abusive est avérée et
    - la personne concernée a été informée par écrit.

Étant donné que la transmission automatisée des données à Apple ne peut pas être désactivée, ces problèmes doivent être indiqués parmi les risques résiduels (cf. point 4.5).

4.8 Authentification et mots de passe

Une authentification à deux facteurs est nécessaire pour les administratrices et les administrateurs. Elle peut être activée gratuitement dans Apple School Manager.

Une authentification à deux facteurs est recommandée pour les membres du corps enseignant. En cas de connexion avec un facteur unique, le risque encouru est considérable étant donné que des tiers peuvent s'emparer illégalement du compte.

Apple School Manager offre trois modes d'authentification :

- Utilisation de l'authentification de l'iCloud

[8] www.belex.sites.be.ch/app/fr/texts_of_law/153.011.5/art/8

- Synchronisation du mot de passe du service d'annuaire interne Azure Active Directory
- Utilisation d'un service d'authentification interne (p. ex. Active Directory Federation Service) via l'interface SAML

Le mode d'authentification doit être défini dans le cadre d'une analyse de risques tenant compte du but et de l'étendue du traitement des données et du type de données traitées.

4.9 Rôles et droit d'accès

Les rôles et droits d'accès octroyés doivent faire l'objet d'un contrôle annuel. Chaque personne doit être autorisée à accéder uniquement aux données dont elle a effectivement besoin.

4.10 Saisie des utilisatrices et utilisateurs

En cas de recours, malgré les recommandations contraires, à des services de *cloud* personnalisés, il convient de tenir compte de ce qui suit :
Apple traite non seulement les données personnelles transmises dans le cadre des services de Cloud (en particulier les données de contenu) mais aussi les données générées par les utilisatrices et utilisateurs ou par ses propres services (par ex. données secondaires de communication, de télémétrie ou de procès-verbal). Ces données personnelles supplémentaires doivent être traitées avec la même diligence que les données servant à l'exécution effective de tâches.

Lors de la saisie des utilisatrices et utilisateurs, il y a donc lieu de renseigner uniquement les informations indispensables (principe du minimum de données nécessaire). Ils doivent aussi être pseudonymisés (p. ex. 149478@ecolexyz.ch).

De nombreuses communes travaillent déjà avec des logiciels qui peuvent être utilisés comme des fournisseurs d'identité (*Identity Provider*, IdP), par exemple :
- Evento
- iCampus
- logiciels du service de contrôle des habitants

Ces fournisseurs d'identité permettent d'exporter la base de données au moyen d'un numéro d'identifiant, qui peut être utilisé pour la pseudonymisation.

4.11 Synchronisation des données des utilisatrices et utilisateurs

Une synchronisation des données des utilisatrices et utilisateurs avec l'iCloud d'Apple n'est possible qu'en tenant compte des informations indiquées au point 4.10.

4.12 Suppression des données

La suppression des données numériques obéit aux mêmes principes que la destruction des documents papier. Les obligations prévues par le canton de Berne en matière de conservation des données s'appliquent. Les données qui ne sont plus utiles doivent être supprimées. Les utilisatrices et utilisateurs doivent avoir la possibilité de transférer leurs données sur un autre support de stockage avant leur suppression.

La suppression des données de procès-verbal s'effectue de manière automatisée.

4.13 Sécurité des données et planification des urgences

Les exigences relatives à la disponibilité d'applications doivent être définies. En cas de besoin, des mesures de sécurité des données et de planification des urgences doivent être mises en œuvre.

4.14 Données de diagnostic

Lors de l'utilisation de matériel Apple, il est possible que des données soient transmises à Apple. Étant donné que les administratrices et administrateurs n'ont aucun moyen de prendre des mesures concernant les données de diagnostic, il leur reste à identifier les risques résiduels.

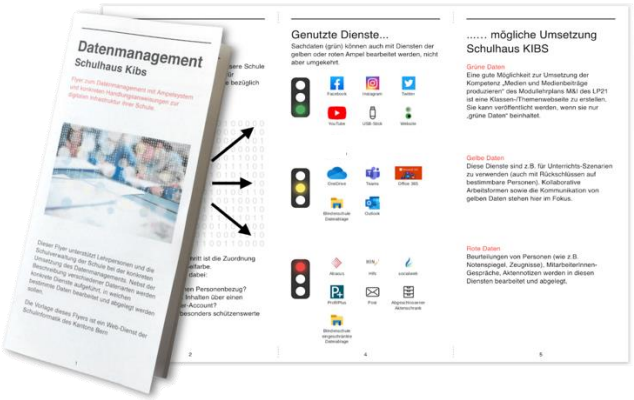
5 Information des personnes concernées

Les utilisatrices et utilisateurs doivent être préalablement informés de l'utilisation prévue de matériel Apple en combinaison avec Apple School Manager dans l'école. Il importe de communiquer les principaux risques encourus et les mesures de protection planifiées.

Les utilisatrices et utilisateurs reçoivent un résumé concernant l'utilisation du matériel Apple en combinaison avec Apple School Manager et d'autres logiciels dans l'école.

Le Conseil en informatique scolaire de la PHBern fournit à cet effet à chaque école un dépliant personnalisable sur le modèle des feux tricolores[9].

Exemple :



5.1 Formation et sensibilisation

Les formations portant sur l'infrastructure et la sensibilisation dans des domaines d'application pertinents pour la protection des données doivent débuter dès le déploiement et l'utilisation de l'infrastructure.

[9] https://kibs.ch/datenschutz

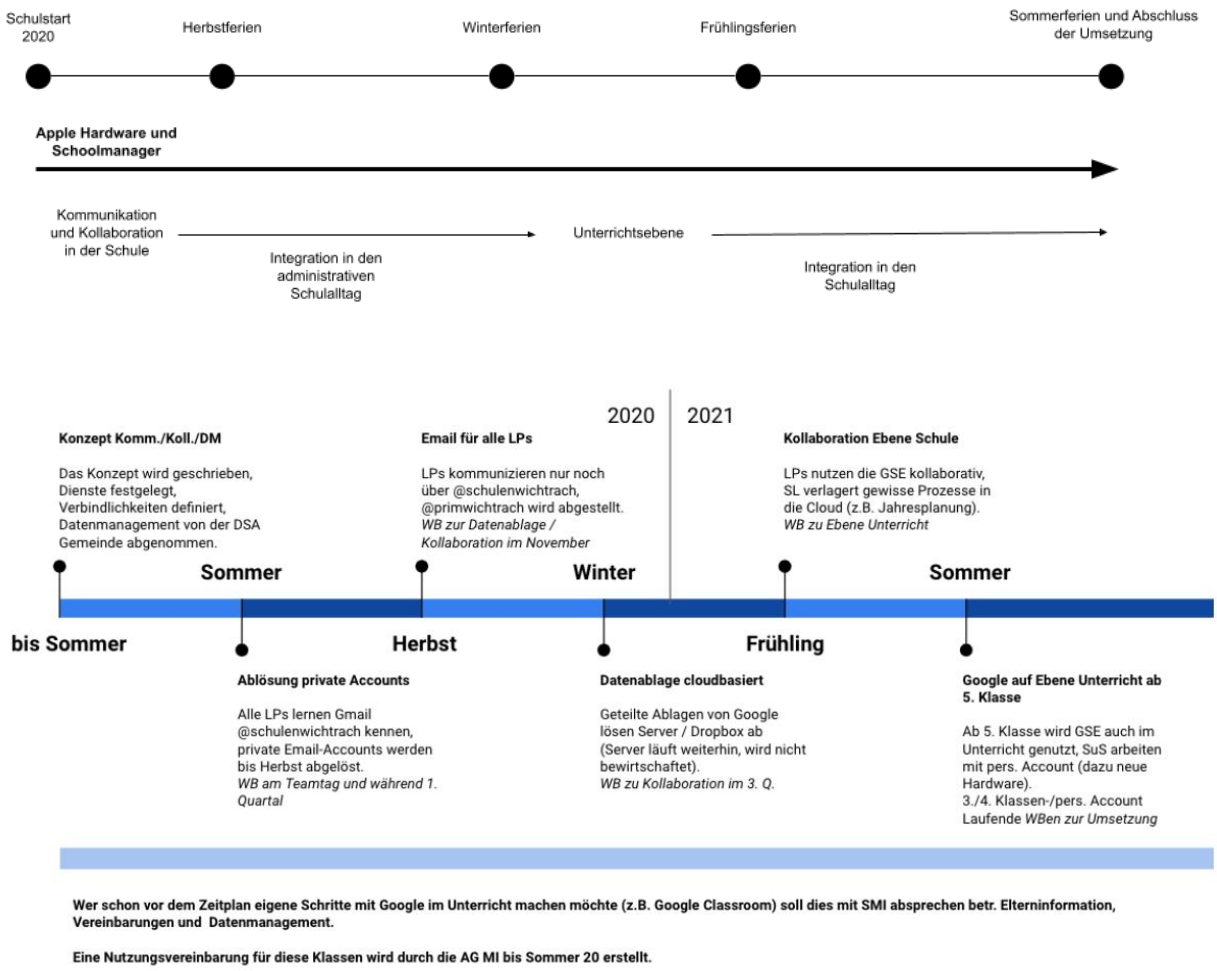
5.1.1 Membres du corps enseignant

Les directives concernant la gestion des données à l'école complètent les mesures de protection techniques (cf. point 4.4 *Exemples*).

Étant donné que les écoles font face à de fortes fluctuations en matière de personnel enseignant (maladie et remplacements), il est impératif de veiller à ce que les enseignantes et enseignants nouvellement engagés puissent obtenir rapidement et facilement les informations essentielles nécessaires à l'utilisation de l'infrastructure informatique scolaire.

Le Conseil en informatique scolaire de la PHBern a constaté par expérience que le perfectionnement continu des membres du corps enseignant dans le domaine de l'infrastructure (par ex. par les spécialistes Médias et informatique, SMI) produisait des effets plus durables qu'une formation unique dispensée par une entreprise externe. Pour décharger les SMI, les écoles peuvent mettre à disposition des processus centraux ou des thèmes liés à la sensibilisation sous forme de documents ou de vidéos.

Exemple de planification de l'introduction du matériel Apple et d'Apple School Manager sur une année



5.1.2 Élèves

La formation des élèves peut avoir lieu dans le cadre de la stratégie de mise en œuvre pour l'enseignement des contenus des plans d'études liés à l'éducation aux médias et à l'informatique.

6 Parents

Les parents doivent être informés à l'avance (avant le déploiement) de l'utilisation prévue du matériel Apple en combinaison avec Apple School Manager.

6.1 Information des parents

Il importe d'informer les parents via plusieurs canaux. D'une part, toutes les stratégies relatives à l'infrastructure ainsi qu'aux médias et à l'informatique (cf. recommandations[10]) doivent être accessibles librement et en toute transparence. D'autre part, les parents doivent avoir la possibilité de poser des questions et d'exprimer leurs réserves.
.

6.1.1 Documents

- Stratégie de mise en œuvre pour l'éducation aux médias et à l'informatique (découlant des recommandations du canton de Berne)[11], exemples de contenus :
    - Enseignement et développement de l'enseignement
    - Développement du personnel
    - Collaboration et communication
    - Gestion des données et aspects juridiques
    - Aspects techniques et financiers
- Stratégie relative à l'infrastructure du Cloud (requise sur la base de la présente notice)

6.1.2 Séance d'information

L'information peut parvenir au parents via plusieurs canaux. D'une part, toutes les stratégies relatives à l'infrastructure ainsi qu'aux médias et à l'informatique doivent être accessibles librement et en toute transparence. D'autre part, les parents doivent avoir la possibilité de poser leurs questions et d'exprimer leurs doutes. Une séance d'information au sujet de l'introduction prévue de l'infrastructure informatique réunissant toutes les personnes concernées (commune, autorité communale de surveillance de la protection des données, direction d'école, SMI, membres du corps enseignant, éventuellement entreprises et/ou PHBern) peut s'avérer particulièrement efficace.

6.1.3 Prise de connaissance

Si Apple School Manager est déployé conformément à la présente notice, on peut partir du principe que les personnes détenant l'autorité parentale sont informées de la mise en œuvre.

[10] Recommandations aux communes et aux directions d'école
[11] kibs.ch, la plateforme du Conseil en informatique scolaire de la PHBern, fournit un soutien.