Kanton Bern
Canton de Berne

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

NOTICE RELATIVE À MICROSOFT 365

Table des matières

1 Introduction

La présente notice est destinée aux services responsables des établissements de la scolarité obligatoire souhaitant utiliser le produit « Microsoft 365 » 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 de Microsoft 365 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 Microsoft 365 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 de Microsoft 365 à l'école obligatoire s'accompagne de risques accrus dans le domaine de la protection des données[1].

Le contrat-cadre conclu avec Educa constitue un instrument important pour réduire ces risques au minimum. Régi par le droit suisse, il stipule que le for juridique est en Suisse et que les serveurs doivent être situés au sein de l'Union européenne ou en Suisse.

Malgré ce contrat-cadre, certains risques demeurent concernant le traitement des données particulièrement dignes de protection et des données secondaires de communication collectées par Microsoft. Une partie de ces risques peuvent être éliminés au moyen de mesures techniques complexes. D'autres risques, dits résiduels, peuvent tout au plus être limités, mais pas supprimés. Ils doivent donc être identifiés et communiqués clairement à l'échelon de direction compétent. La direction peut et doit accepter les risques résiduels qu'elle juge tolérables (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.

4 Stratégie

Avant d'introduire et d'utiliser Microsoft 365, 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].

[1] Cf. nouvelle version révisée de l'aide-mémoire « Risques et mesures spécifiques au cloud » de privatim.
[2] Le Conseil en informatique scolaire de la PHBern aide les écoles à élaborer une stratégie d'utilisation du Cloud.

Ce faisant, il convient de tenir compte en particulier des points suivants :

- 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 de Microsoft 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 ?
- Indication 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 Microsoft 365 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 de Microsoft 365, 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 avec affectation à des buts précis (liste non exhaustive) :

	Scénario	**Personnes concernées**	**Produits/données**
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	Organisation de contrôles des connaissances	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	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 : définition du besoin de protection

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 les scénarios 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	Description
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 relevant du secret professionnel ou de fonction.

Exemple de classifications dans la stratégie :

[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), http://www.belex.sites.be.ch/app/fr/texts_of_law/432.271.1
[4] https://kibs.ch/datenschutz/ampelsystem
[5] RSB 152.17.

	Scénario	Personnes concernées	Produits/données	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 adolescents, personnes détenant l'autorité parentale	Documents, courriels	Confidentiel

[6] Cf. OMO.

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

Microsoft 365 offre une large palette de services. Le choix des services dépend des besoins de l'école (point. 4.1). À noter toutefois que seuls les services couverts par le contrat-cadre peuvent être utilisés.

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 de Microsoft. Le cas échéant, il y a lieu d'inclure dans la stratégie d'autres applications spécialisées compatibles avec le traitement de données confidentielles.

Les possibilités de cryptage décrites au point 4.6 autorisent le traitement de données personnelles de la catégorie « confidentiel » dans Microsoft 365.

Exemple de services retenus dans la stratégie :

Classification des données	**Service choisi**
Public et interne	Microsoft 365 Word, PowerPoint, Excel, OneDrive, Teams, Outlook
Confidentiel	Évaluation21, l'application d'évaluation du canton de Berne[7] (contrôle préalable par la commune non nécessaire) Lehreroffice, Tresorit, Protonmail, Klapp, Threema, Scolaris, etc. (nécessité d'un contrôle préalable par la commune)

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 ».

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

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 : mesures techniques et organisationnelles
- 8 à 16 : choix d'une application spécialisée spécifique ou mise en œuvre de mesures techniques et organisationnelles (au niveau de l'école) supplémentaires.

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 (exemples divers dans la perspective de l'école)
2.a	Produit : contrôles des connaissances, y c. évaluations (prédicat/notation) Les résultats sont divulgués dans l'école.	2	3	6	Les membres du corps enseignant sont formés à ne pas faire figurer les 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	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] ». Un mode d'authentification à deux facteurs est requis pour utiliser l'application spécialisée.
7.a	Élaboration de projets pédagogiques dans le domaine de l'intégration ainsi que mesures de pédagogie spécialisées ordinaires et mesures de soutien relevant de l'offre ordinaire de l'école obligatoire (MO, anciennement IMEP), et sauvegarde dans OneDrive Les administratrices et administrateurs de Microsoft peuvent avoir accès à ces données. Il n'existe aucune possibilité de	3	4	12	Le processus de « Customer Lockbox » empêche les accès non autorisés à ces données. Il existe aussi une fonctionnalité qui, en cas d'utilisation d'un nombre élevé de mots-clés, active automatiquement l'étiquette de sensibilité (« *sensitivity label* ») au niveau correspondant, en l'espèce crypte les données à l'aide de la clé de l'école. La gestion de cette fonction de sécurité au niveau des documents sera précisée et expliquée aux utilisatrices et utilisateurs lors des formations planifiées.

	contrôler si les autorités américaines consultent ces données (en vertu du *CLOUD Act*).				Les membres du corps enseignant utilisent un mode d'authentification à deux facteurs. Autre possibilité : les enseignantes et enseignants élaborent les projets pédagogiques sur leur ordinateur, dans un programme de traitement de texte différent de Word, puis les sauvegardent dans l'application spécialisée spécifique.
7.b	Les projets pédagogiques sont envoyés par courriel à la direction d'école ou aux personnes détenant l'autorité parentale. Lors de la saisie d'une adresse électronique, le risque d'erreur est élevé. 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
8	Oubli du mot de passe Une administratrice ou un administrateur peut réinitialiser en tout temps les mots de passe des utilisatrices et utilisateurs, voire donner à ces derniers l'accès aux données concernées. Les listes de mots de passe comportent un risque de piratage des comptes.	2	3	6	Le rôle d'administratrice ou d'administrateur est inscrit dans le plan des rôles et des droits d'accès. Une convention supplémentaire réglemente les droits et les obligations. Les utilisatrices et utilisateurs reçoivent un mot de passe par défaut et doivent en créer un nouveau à leur prochaine connexion.

4.5 Identification des risques résiduels

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).

Risques résiduels liés au contrat :

- Impossibilité de contrôler l'accès aux données par Microsoft ou des sous-traitants de Microsoft
- 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 pouvant être 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
- Communication des données télémétriques à des sous-traitants aux États-Unis autorisée dans une clause du contrat-cadre avec Educa
- Saisie des noms et prénoms des utilisatrices et utilisateurs (risque de profilage)
- Modifications de contrat unilatérales par Microsoft

Risques résiduels liés à l'organisation de l'école :

- Gestion des mots de passe des élèves du premier cycle par l'enseignante ou l'enseignant compétent pour la classe

- Risque que les commentaires concernant les travaux des élèves contenus dans un même document soient interprétés comme une évaluation formative

4.6 Cryptage

Lors de l'utilisation de Microsoft 365, les données transmises et sauvegardées sont cryptées conformément aux normes applicables en la matière (données en transit [« *data in transit* »] et données au repos [« *data at rest* »]). Microsoft, qui dispose de la clé correspondante, peut en principe accéder aux données cryptées se trouvant sur le Cloud. Les données en cours de traitement dans le Cloud (« *data in process* ») ne sont pas cryptées.
Il est possible de limiter le risque d'accès non autorisé à des données par les employées et employés de Microsoft (ou des entreprises sous-traitantes concernées) en activant le processus de « Customer Lockbox » ou en utilisant une clé propre aux autorités (par ex. pour le traitement de données confidentielles).
Le processus de « Customer Lockbox » peut être activé via l'abonnement A5 de Microsoft. Microsoft s'engage alors par contrat à n'utiliser la clé qu'avec le consentement exprès de l'autorité. Le nom de la collaboratrice ou du collaborateur habilité au sein de l'école à accorder ce consentement doit figurer dans le document définissant les rôles et les droits d'accès.
Il n'est toutefois pas encore exclu que les autorités américaines puissent accéder aux données enregistrées en vertu du *CLOUD Act*.
Dans ce cas, Microsoft offre la possibilité d'utiliser une clé propre à l'autorité (école/commune). La mise en œuvre de cette mesure (dite « *Hold Your Own Key* » ou HYOK) est toutefois exigeante sur le plan technique.

Lors du traitement de données confidentielles dans Outlook, il convient de veiller à ce que la norme S/MIME soit appliquée pour la signature des courriels. Compte tenu des nombreux courriels échangés entre les écoles et des destinataires ou expéditeurs externes, le cryptage S/MIME ne s'applique que dans certains scénarios d'utilisation.

Des solutions de sauvegarde des données ou de courriel utilisant les technologies de sécurité les plus puissantes sont par ailleurs disponibles sur le marché. Le cas échéant, il importe de vérifier que l'entreprise a son for juridique en Suisse et que les serveurs sont situés en Suisse ou au sein de l'UE, et de veiller à la convivialité d'utilisation dans le contexte scolaire. Des exemples sont disponibles sur le navigateur d'Educa.

4.7 Procès-verbal

Lors de l'utilisation de Microsoft 365, des données relatives aux utilisatrices et utilisateurs et leurs activités peuvent être automatiquement consignées et sauvegardées (données de connexion).

Une évaluation de ces données de connexion n'est possible que dans des conditions précises (cf. ordonnance cantonale sur les données secondaires de communication (ODSC) :

- 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.

La transmission automatisée de données de diagnostic à Microsoft doit être désactivée
(cf. point 4.14 *Données de diagnostic*).

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 Microsoft 365.
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.

Microsoft 365 offre trois modes d'authentification :

- Utilisation de l'authentification Microsoft 365 intégrée
- Synchronisation du mot de passe du service d'annuaire interne Active Directory (ou Azure AD) avec Microsoft 365 (ou Azure AD)
- Utilisation du service d'annuaire interne Active Directory Federation Service (ADFS)

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

Microsoft 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).
Lorsque les données sont saisies explicitement dans le Cloud, aucun autre attribut en dehors du nom ne peut être indiqué.
En cas de doute ou sur demande, la pseudonymisation des données doit être proposée.

4.11 Synchronisation des données des utilisatrices et utilisateurs

Une synchronisation des données des utilisatrices et des utilisateurs avec le Cloud de Microsoft (y c. avec les serveurs aux États-Unis) est nécessaire dans certains cas de figure. Les données suivantes sont notamment concernées :

- Service de réinitialisation de mot de passe (SSPR)
- Authentification à deux facteurs
- Activation de licences

Seules les données d'utilisatrices et d'utilisateurs impérativement nécessaires peuvent être transmises. Il en va de même pour les attributs, y compris en cas de recours à un fournisseur d'identité (*Identity Provider*, IdP). Exemple : utilisation d'une plateforme Azure Active comme fournisseur d'identité pour le raccordement à Edulog.

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. Les délais de conservation sont indiqués sur la page suivante : https://learn.microsoft.com/fr-ch/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview.

4.13 Sécurité des données et planification des urgences

Les exigences relatives à la disponibilité de Microsoft 365 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

Les données transmises à Microsoft diffèrent selon que l'on utilise Microsoft 365 Pro Plus en local sur son ordinateur ou sa version mobile (pour tablettes ou smartphones). Il appartient aux administratrices et administrateurs de prendre des mesures en conséquence.

Il faut en particulier veiller aux points suivants :

- Toujours utiliser les versions actuelles
- Activer l'option « ni l'un ni l'autre » pour les données de diagnostic
- Configurer les « expériences connectées facultatives » et si possible les désactiver de manière centralisée
- Désactiver la participation au programme d'amélioration de l'expérience utilisateur (« Microsoft Customer Experience Improvement Program », CEIP)

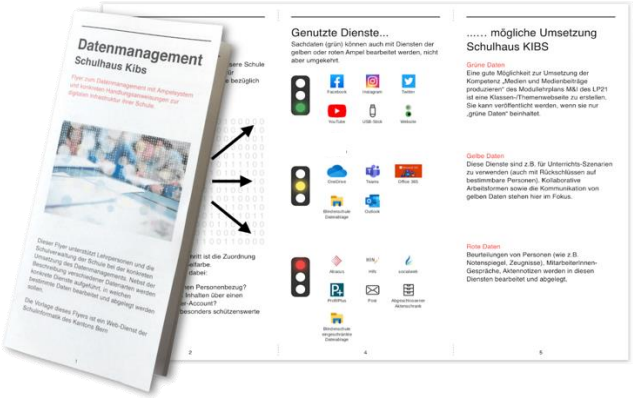
5 Information des personnes concernées

Les utilisatrices et utilisateurs doivent être préalablement informés de l'utilisation prévue de Microsoft 365 dans l'école. Il importe de communiquer les principaux risques encourus et les mesures de protection planifiées.

Les utilisatrices et utilisateurs reçoivent une liste des services de Microsoft 365 dont dispose l'école et de leurs modalités d'utilisation.

Le Conseil en informatique scolaire de la PHBern fournit à cet effet à chaque école un dépliant personnalisable sur le modèle des feux tricolores[8].

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.

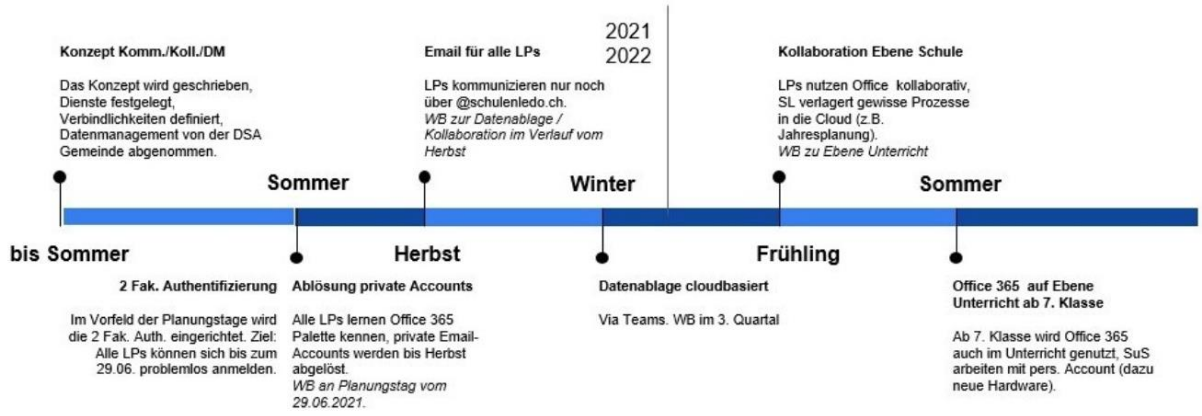
5.1.1 Membres du corps enseignant

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, 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.
C'est également là que le dépliant personnalisable avec les feux tricolores mis au point par le Conseil en informatique scolaire de la PHBern entre en jeu.

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.
Les processus centraux concernant l'utilisation ou les thèmes liés à la sensibilisation sous forme multimédia peuvent soutenir les membres du corps enseignant et décharger les SMI.

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

Exemple de planification de l'introduction de Microsoft 365 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 de Microsoft 365.

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[9]) doivent être accessibles librement et en toute transparence. D'autre part, les personnes détenant l'autorité parentale 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)[10], 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)

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

6.1.2 Séance d'information

Il est essentiel que l'école ou la commune communiquent au sujet du traitement des données personnelles en organisant une séance d'information destinée aux parents, et ce avant la mise en place de l'infrastructure.

Lors de cette séance, en plus des informations générales, il conviendra de préciser les enseignements concernés (contenus du plan d'études liés aux médias et à l'informatique). Dans l'idéal, toutes les parties prenantes participant aux travaux stratégiques devraient être présentes (commune, autorité communale de surveillance de la protection des données, direction d'école, SMI, membres du corps enseignant, éventuellement entreprises et/ou PHBern).
La séance contribuera ainsi à dissiper les doutes et à satisfaire les demandes.

6.1.3 Prise de connaissance

Si Microsoft 365 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.

7 Annexes

7.1 Principaux services de Microsoft 365 selon les contrats-cadres (vue d'ensemble)

Source : guide d'utilisation de Microsoft 365 dans le domaine éducatif (en allemand uniquement) publié par le service responsable de la protection des données du canton de Zurich.

Service	Descriptions	Autre possibilité locale
Azure Active Directory	Gestion ou représentation des identités	
Bookings	Outil de simplification de la planification et de la gestion des rendez-vous Exemple : entretien avec les parents	
Classroom Tools	Différents services, applications et fonctionnalités utiles pour l'école : outils d'apprentissage, de suivi des progrès et de coaching en lecture, de contrôle de l'accessibilité, application « Take a Test », application « Set up School PCs »	
Compliance	Différents services et fonctionnalités, par ex. gestion des droits, protection des informations, prévention de la perte de données, conformité des communications, cryptage, « Customer Lockbox », etc.	
Delve	Analyse et visualisation de son utilisation personnelle et mise en évidence dans Microsoft 365 des documents et informations intéressants pour les utilisatrices et utilisateurs	
Exchange / Exchange Online	Courriel, calendrier, contacts, tâches	X
Flow	Outil d'automatisation des processus d'affaires permettant de créer des flux opérationnels automatisés entre des applications et des services, de recevoir des messages, de saisir et de synchroniser des données, etc.	
Forms	Outil de création de formulaires	

	Exemple : contrôles des connaissances (met en évidence les réponses fausses)	
Groups	Création de groupes d'utilisatrices et utilisateurs afin de partager des contenus provenant de différents services	
Intune / Intune for Education	Installation et gestion des appareils	
Lists	Création, validation et suivi de listes Exemple : planification de la fête de l'école	
Microsoft 365 Apps for Enterprise	Applications Office installées, par ex. Word, PowerPoint ou Outlook, qui favorisent la productivité	
Minecraft: Education Edition with Code Builder	Version éducative du jeu basé sur des blocs : scénarios se déroulant dans l'environnement scolaire, notamment en vue de l'apprentissage de la programmation.	
Office 365 pour le web	Environnement Office 365 en ligne, autrement dit l'environnement cloud de l'école : cadre de mise à disposition de nombreux services, de la gestion des entités (« *Tenant Administration* ») ainsi que des versions web des applications Office.	
OneDrive for Business	Espace personnel de stockage de documents	X
OneNote	Bloc-notes Exemples : préparation de l'enseignement, tableau noir électronique, etc.	X
OneNote Class Notebook	Bloc-notes pour la classe offrant des fonctionnalités additionnelles Exemples : distribution de fiches de travail aux élèves, simplification de la correction de devoirs à la maison, etc.	
Phone	Complément payant de Teams pour la téléphonie Exemples : téléphonie Teams pour la classe, l'accueil extrascolaire, etc.	
Planner	Outil de travail en équipe Exemples : création de plans, organisation et attribution de tâches, validation de données, discussion de tâches dans le chat, échange, etc.	
PowerApps	Création d'applications d'affaires définies par l'utilisatrice ou l'utilisateur	
Power Automate	Création de flux opérationnels entre applications, données et fichiers afin d'automatiser des tâches chronophages Exemples : dépôt, approbation et archivage d'une demande d'acquisition	
PowerBI	Business Intelligence. Compilation d'outils pour l'analyse et la visualisation de données enregistrées sur SharePoint et le partage de résultats	
Project / Project Online	Outil complet de gestion de projet	X
School Data Sync	Service de Microsoft 365 pour les établissements de formation capable de lire les listes des élèves et des services du système d'information scolaire de l'école	

	Permet de créer automatiquement des groupes Microsoft 365 pour Exchange Online et SharePoint Online, des équipes « classes » sur Teams et des blocs-notes sur OneNote pour la classe	
SharePoint / SharePoint Online	Espace de stockage de documents partagé avec d'autres utilisatrices et utilisateurs au sein de groupes prédéfinis (cf. « Groups »)	X
Sécurité	Divers services et fonctions pour sécuriser les données et l'environnement Exemples : Microsoft Defender for Office 365 / for Cloud Apps / for Endpoint, Antivirus, Advanced Threat Analytics, etc.	
Skype for Business	Fonctions de *chat*, de téléphonie, de visioconférence, de partage d'écran et d'applications, etc. Seules les discussions via le *chat* (sur le serveur Exchange), et non les conversations téléphoniques, sont enregistrées. Les conversations en visioconférence peuvent être enregistrées et stockées sur SharePoint.	(X)
Stream	Plateforme de vidéos interne à l'école : enregistrement, recherche et partage de vidéos	
Teams / Classroom experiences dans Teams	Environnement de travail dans Microsoft 365 basé sur le *chat*. Combinaison de services Microsoft 365 axés surtout sur l'interaction au sein d'équipes Exemple : combinaison de Skype, SharePoint et OneNote	
To Do	Service intégré à Microsoft 365 pour faciliter la gestion des tâches et l'organisation de la journée	
Visio	Outil permettant de simplifier visuellement et de transmettre des informations complexes Exemples : organigrammes, diagrammes	
Viva Connections	Plateforme basée sur Sharepoint destinée aux établissements scolaires qui facilite la communication, l'échange et la mise en réseau Exemples : Intranet, page d'accueil interne	
Viva Insights	Amélioration de la productivité	
Viva Learning	Offre la possibilité d'intégrer facilement l'accès à des contenus d'apprentissage, de suivre les progrès d'un cours, de les partager, etc. (corps enseignant uniquement) Exemples : cours Teams pour les membres du corps enseignant, formation des utilisatrices et utilisateurs d'applications spécialisées	
Whiteboard / Whiteboard in Teams	Développement collaboratif de projets de dessin sur tableau blanc Exemples : travaux de groupe, brainstorming	

7.2 Autres services inclus dans les contrats-cadres (extrait)

Service	Description
Plateforme Azure Cloud	Infrastructure en tant que service (IaaS) : machines virtuelles, réseau, stockage Plateforme en tant que service (PaaS) : banque de données, Intelligence and Analytics Logiciel en tant que service (SaaS) : applications d'affaires

Dynamics 365	Gestion des relations clients (CRM) et planification des ressources (ERP) Services de gestion des ressources (comptabilité, gestion du personnel, des élèves, des contrats, des stocks, etc.) Exemple : historique des appels de clients
EMS E3 for Intune	Composants pour le pilotage des identités et des accès dans le Cloud ainsi que la gestion des appareils mobiles et des applications Exemple : assurer la mise à jour de l'ensemble des ordinateurs portables de l'école et la protection contre les accès non autorisés
Intune	Gestion des applications et des appareils
Intune for Education	Offre une surface d'utilisation simplifiée par rapport à Intune. Ce service peut être utilisé de manière autonome ou en complément de l'environnement complet d'Intune pour la gestion des appareils.
Infrastructure et serveurs	Serveurs de productivité tels que Exchange, SharePoint, SQL, etc.

7.3 Services non couverts par les contrats-cadres

Les services suivants ne peuvent être utilisés conformément à la législation sur la protection des données, notamment car ils stockent tout ou partie des données en dehors de l'UE.

Service	**Description**
OneDrive (version consommateur)	Stockage de documents privés Le seul espace de stockage que les écoles peuvent utiliser conformément à la législation sur la protection des données est OneDrive for Business (cf. point 9.1).
Skype (version consommateur)	Communication : *chat*, téléphonie, partage d'écran, etc. Les seuls outils de communication que les écoles peuvent utiliser conformément à la législation sur la protection des données sont Teams et Skype for Business (cf. point 9.1).
Sway	Outil de création de présentations en ligne fonctionnant comme un site Internet
Yammer	Réseau social pour les entreprises