Workshop du 24 mai 2017 sur la protection des données

Cas 1 : Page Facebook d'un établissement scolaire

Un établissement scolaire a ouvert une page sur le réseau social Facebook. Sur cette page, on voit notamment une photo d'une dizaine d'élèves qui assistent au discours de Saint-Nicolas. Dans les commentaires, un parent d'élève fait une remarque en y citant le nom de son enfant.

Liens avec la directive :

Articles 3, 4, 6, 7, 10 et 15

Commentaire :

L'utilisation d'un réseau social comme ici Facebook n'est pas optimale si elle n'est pas faite dans un but pédagogique. Nous conseillons de ne pas le faire à des fins de communication extérieure ou à des fins de promotion. Une page sur Facebook est aussi potentiellement susceptible d'afficher des commentaires des parents où ils publient des données personnelles, ce qui est très difficile à contrôler.

Modifications nécessaires dans le cas d'espèce :

Il faudrait retirer la page Facebook de l'établissement ou du moins retirer la photo où l'on voit les enfants (le commentaire de la maman devrait aussi être retiré).

Cas 2 : Film publié sur YouTube pour promouvoir une école

Un établissement scolaire a réalisé un film pour promouvoir son établissement. Ce film a été mis sur la plateforme YouTube et intégré sur le site web de l'établissement. Sur ce film, on voit très distinctement le visage des élèves.

Liens avec la directive :

Articles 3, 4, 6, 10, 12 et 15

Commentaire :

Le site web d'une école ne devrait pas être une plateforme de promotion mais bien d'échanges d'informations ou d'éléments de nature pédagogique.

La publication d'un film incluant des données personnelles nécessite le consentement de chaque personne filmée.

Il n'est pas permis de poster sur YouTube un film incluant de telles données. Il est possible de le faire avec une plateforme telle que Scolcast par exemple.

Enfin, ces données personnelles doivent être sous couvert d'un mot de passe communiqué aux personnes autorisées à accéder à ces données.

Modifications nécessaires dans le cas d'espèce :

Il est important de préciser les éléments suivants :

- Si chaque intervenant a donné son consentement (ou ses parents s'il est mineur), il serait possible de mettre ce film sur la page web de l'école, mais en aucun cas sur YouTube.
- Dans le cadre d'un film promotionnel, il serait préférable de faire intervenir un acteur externe à l'établissement. En effet, si l'on filme des élèves actuellement scolarisés dans l'école, on doit flouter leurs visages ou faire des plans de loin pour que ces personnes ne soient pas reconnaissables.
- La durée de publication du film doit se limiter à quelques mois (le temps que dure la promotion).

Cas 3 : Photo et nom/prénom d'un-e élève sur le site d'un camp polysportif

Une école a créé un site dédié à son camp polysportif. Pour le rendre attractif, cette école a mis les photos des élèves sous la forme d'un diaporama aux couleurs de la thématique du camp. Sous ce diaporama, où l'on voit distinctement les visages des élèves, sont mentionnés les noms des élèves.

Liens avec la directive :

Articles 3, 4, 10 et 12

Commentaire :

De manière générale, s'il est possible de reconnaître clairement les élèves sur une photo (donnée personnelle), il convient de la publier dans une zone du site web protégée par un mot de passe. Ces mots de passe ne doivent en aucun cas être distribués à large échelle. Le contrôle de leur distribution incombe à la direction de l'établissement. Le consentement explicite des parents pour cette publication est bien entendu obligatoire.

Modifications nécessaires dans le cas d'espèce :

La partie de ce site web qui présente des galeries photos ou des données personnelles doit être accessible via un mot de passe à donner aux parents et aux moniteurs du camp par exemple. Ces photos doivent être supprimées une fois le camp terminé. Si les enseignant-e-s veulent garder des archives, il convient de ne pas les mettre sur le web (y compris dans la partie sécurisée), mais de les conserver sur un ordinateur de l'école (ou le serveur interne de l'école).

Cas 4 et 5 : Photo d'élèves ayant gagné un concours dans le cadre scolaire ou ayant participé à une représentation théâtrale/musicale

Sur le site web d'une école, on peut voir les images des vainqueurs d'un concours interne à l'école et des photos présentant une troupe de théâtre/un ensemble musical avec les noms des vainqueurs/acteurs-trices/musiciens-ciennes.

Liens avec la directive :

Articles 3, 4, 10 et 12

Commentaire :

S'il ne s'agissait pas d'un concours ou de représentations artistiques, ces photos et données personnelles devraient être mises dans une zone sécurisée avec accès conditionné par un mot de passe. Dans ce cas précis, les élèves ayant gagné un concours ou participé à des

représentations artistiques, on peut accepter de mettre cette photo sur le site web. Cela doit par contre respecter deux règles :

- Chaque élève (ou son représentant légal) doit donner son consentement à la publication de ces photos.
- Les photos doivent être supprimées 3 mois après la fin du concours/concert/spectacle et peuvent être conservées dans les archives sur le serveur de l'école.

Cas 6 : Productions d'élèves nominatives sur le site internet de l'établissement scolaire

Des productions d'élèves figurent sur le site web d'une école. Ces productions, issues d'un concours de dessin, sont publiées avec le nom de l'élève-auteur ainsi que la classe dans laquelle il est.

Liens avec la directive :

Articles 3, 10 et 12

Commentaire :

La publication de travaux d'élèves est soumise au droit d'auteur que nous ne traiterons pas ici. La problématique, en matière de protection des données, n'est ici pas le fait de publier les dessins mais les données personnelles de l'élève avec son prénom, son nom et l'indication de sa classe.

Modifications nécessaires dans le cas d'espèce :

Les dessins peuvent rester publiés (avec le consentement des auteurs), mais il faut retirer les données personnelles qui y figurent (en laissant uniquement le prénom par exemple).

Cas 7 : Les coordonnées des enseignants du cercle scolaire mises en ligne et accessibles par tous

La direction d'établissement, ou la Commune, a mis en ligne les coordonnées des enseignant-e-s du Cercle scolaire. Ces coordonnées comprennent les numéros de téléphone ainsi que les adresses privées des enseignant-e-s.

Liens avec la directive :

Articles 3, 5, 10 et 12

Commentaire :

Pour le personnel enseignant, les données suivantes peuvent être publiées sur le web : nom, prénom, fonction, disciplines enseignées, adresse de courriel professionnelle. Toute publication supplémentaire (adresse privée, numéro de téléphone privé, etc.) nécessite le consentement explicite et volontaire de la personne concernée.

Modifications nécessaires dans le cas d'espèce :

Si une école veut mettre en ligne les coordonnées privées du corps enseignant, elle doit en premier lieu demander le consentement de chacun. Ces coordonnées devraient en principe être dans une zone sécurisée et accessible via mot de passe distribué par la Direction de l'établissement. Ces coordonnées seraient supprimées à la fin de l'année scolaire.

Il faut toutefois indiquer que certaines données **professionnelles** d'enseignant-e-s peuvent être publiées, à savoir nom, prénom, fonction, disciplines enseignées, adresse de courriel professionnelle.

Cas 8 : L'équipe enseignante partage des observations d'élèves sur Evernote, Azendoo, Google Drive, etc.

Les enseignant-e-s décident de partager des informations personnelles et confidentielles via des plateformes ne respectant pas la législation en matière de protection des données (par exemple des information sur le comportement des élèves, justification des absences, liste de classe, …).

Liens avec la directive :

Article 6

Commentaire :

Le partage de documents sur ce genre de plateforme est tout à fait autorisé - à condition qu'ils ne comportent pas de données personnelles et sensibles. Si de telles données sont stockées sur le web, elles doivent précisément passer par la plateforme officielle fribox mise en place par la Direction de l'instruction publique.

Modifications nécessaires dans le cas d'espèce :
Les données personnelles qui sont citées sur la plateforme doivent disparaitre. La plateforme fribox doit être utilisée pour ce genre d'usage.

Cas 9 : Un-e enseignant-e crée un groupe WhatsApp pour des communications avec les parents.

Un-e enseignant-e décide de communiquer des informations aux parents relatives à l'organisation d'activités de la classe au moyen d'un groupe WhatsApp.

Liens avec la directive :
Article 7

Commentaire :
La communication avec les parents doit se faire par les canaux « officiels » et conventionnels. Par là, on entend le courriel, le téléphone ou encore la circulaire écrite. Une application telle que WhatsApp ne respecte pas la protection des données, non pas par le contenu des messages mais par la récolte et la diffusion automatique des méta-données de l'utilisateur-trice (numéro de téléphone, informations du carnet d'adresse, etc.).
Toutefois demeurent réservées les camps, les activités hors du périmètre de l'école, etc. Dans ce cas-là (et par le fait que dans ces cas les personnes doivent parfois être atteintes rapidement ou de manière urgente), il est autorisé d'utiliser WhatsApp et de créer un tel groupe. Ce dernier devra être supprimé une fois l'activité terminée.

Modifications nécessaires dans le cas d'espèce :
Dans ce cas précis, l'enseignant-e devrait communiquer ces informations « non-urgentes » par un autre canal.

Cas 10 : L'enseignant-e demande aux parents l'autorisation de vérifier le contenu de la messagerie d'école de leur enfant. Peut-il le faire ?

Un-e enseignant-e a fourni aux élèves de sa classe des adresses de courriel pour réaliser un projet pédagogique. Malheureusement les élèves s'envoient des messages injurieux par courriel. Pour résoudre le problème, l'enseignant-e demande aux élèves d'avoir accès aux comptes de courriel.

Liens avec la directive :

Article 7

Commentaire :

L'enseignant-e peut fournir à ses élèves une adresse de courriel educanet2. Cette boîte courriel est un outil de classe qui ne doit être utilisé qu'à des fins pédagogiques dans le cadre d'un projet. L'accès à cette boite aux lettres est possible pour les parents des élèves, et ce jusqu'à la majorité de leur enfant. Pour ce qui est des enseignant-e-s, il est possible également d'avoir accès à ces informations dans le cas où les circonstances les y obligent. Pour consulter le contenu du compte de courriel des élèves, l'école devra faire une demande écrite aux parents.

Modifications nécessaires dans le cas d'espèce :

Dans ce cas précis, l'enseignant-e devra faire la demande aux parents d'élèves pour avoir accès au compte de courriel des élèves de la classe.

Cas 11 : La Direction informe les parents d'une sanction disciplinaire par courriel.

Quelques élèves de l'école ont gravement contrevenu aux règles de l'école et la Direction en informe les parents par courriel.

Liens avec la directive :

Article 7

Commentaire :

De manière générale, il faut considérer la communication par courriel comme non-sécurisée. On pourrait l'apparenter à une carte postale, donc très facilement lisible par des tierces personnes. La communication de données sensibles aux parents doit se faire par courrier postal ou par téléphone s'il y a urgence (avec un courrier qui peut être transmis si la trace écrite est nécessaire).

Modifications nécessaires dans le cas d'espèce :

Les communications comportant des données personnelles entre les enseignant-e-s de l'école ou entre les différents professionnels de l'école ne devraient **en principe** pas se faire par courriel. Dans la pratique cela peut être assez compliqué ; donc le principe de proportionnalité admet cela si la communication par un autre biais que le courriel est impossible ou demande des moyens disproportionnés. A l'avenir, les documents contenant des données personnelles ne devraient plus transiter en pièce jointe mais être déposés dans un dossier partagé fribox.

Cas 12 : Une école a publié un document contenant des instructions sur le camp de ski.

L'établissement a protégé le site Internet du camp avec un mot de passe. Ce mot de passe est publié sur le site de la Commune dans un fichier PDF accessible à n'importe qui.

Liens avec la directive :

Article 12

Commentaire :

Il est juste de mettre des documents contenant des données personnelles (photos, vidéos, etc.) dans la partie sécurisée du site web. Par contre, il est important de ne **jamais** divulguer le mot de passe sur un site web ouvert ! Ce mot de passe doit être uniquement distribué aux personnes ayant un droit d'accès à ces données.

Modifications nécessaires dans le cas d'espèce :

Dans ce cas précis, il faut enlever le mot de passe du document.

Cas 13 : Sur la page Facebook d'une école figure une photo de l'ensemble des enfants de l'école.

Cette photo publiée sur Facebook est téléchargeable en haute définition et permet de reconnaitre distinctement chaque élève.

Liens avec la directive :

Articles 3, 4, 6, 7, 10 et 15

Commentaire :

Outre les commentaires du cas 1 qui s'appliquent aussi ici, il est important de mentionner que sur le site d'une école peuvent figurer les photos de groupe (et ce même dans la partie non-sécurisée du site web). Toutefois la qualité de la photo ne doit pas permettre de reconnaitre **individuellement** les élèves.

Modifications nécessaires dans le cas d'espèce :

Comme pour le cas 1.

Cas 14 : Sur sa page Facebook privée, un enseignant a posté une photo obscène, insultante, etc.

Liens avec la directive :

Article 16

Commentaire :

L'enseignant-e peut bien entendu utiliser Facebook à titre privé et ce conformément au Guide d'utilisation des réseaux sociaux par les collaborateurs-trices de l'Etat. Cela dit, il est particulièrement important de rendre attentif les enseignant-e-s que les informations qu'ils publient sur Facebook sont susceptibles d'être lues par des personnes externes à leur sphère privée. Des publications à caractère obscène, insultantes ou autres peuvent nuire à leur réputation d'enseignant-e et doivent être bannies. Le collaborateur-trice qui publie du

contenu qui pourrait nuire à l'image de son employeur-euse ou de ses collègues est susceptible de sanctions graves (qui peuvent aller jusqu'au licenciement).

Modifications nécessaires dans le cas d'espèce :

Retirer la photo de la page Facebook.