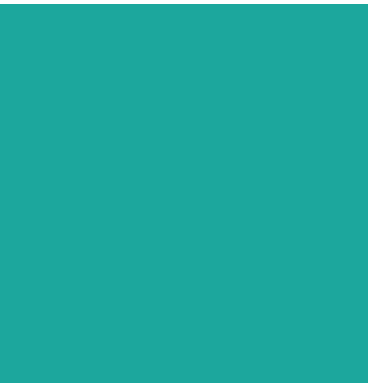
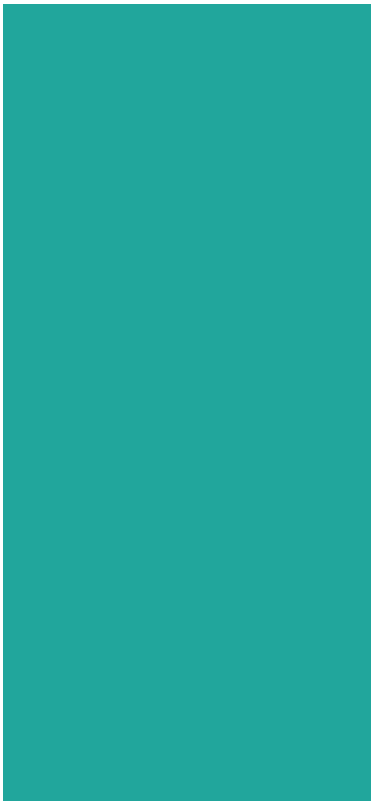
FÉDÉRATION
WALLONIE-BRUXELLES
ENSEIGNEMENT.BE

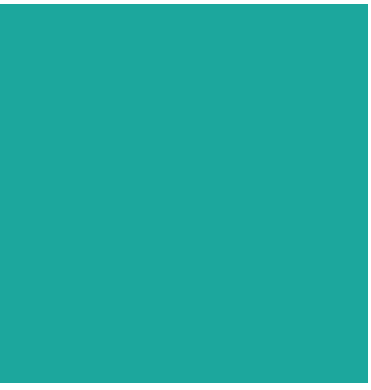
Pacte pour un
Enseignement
d'excellence

GUIDE PRATIQUE

La cybersécurité pour les écoles







Réalisé par l'Administration générale de l'Enseignement
Service général du Numérique éducatif

FÉDÉRATION WALLONIE-BRUXELLES
ENSEIGNEMENT.BE

Pacte pour un Enseignement d'excellence

ETNIC
LE PARTENAIRE INFORMATIQUE DU PROGRÈS EN FÉDÉRATION WALLONIE-BRUXELLES

CENTRE FOR CYBER SECURITY BELGIUM

GUIDE PRATIQUE

La cybersécurité pour les écoles

Ce guide a été rédigé par le Service général du Numérique éducatif (SGNE) de la Fédération Wallonie-Bruxelles, dans le cadre du Pacte pour un Enseignement d'excellence.

Avec la participation de l'Entreprise des Technologies Numériques de l'Information et de la Communication (ETNIC), le partenaire informatique de la Fédération Wallonie-Bruxelles.

Et avec l'appui du Centre pour la Cybersécurité Belgique (CCB), l'autorité nationale en charge de la cybersécurité en Belgique.

TABLE DES MATIÈRES

(1) Les mots-clés suivis du symbole « ? » sont définis dans le glossaire.

I INTRODUCTION

De nombreux établissements scolaires de la FW-B établissent graduellement leur **écosystème numérique** ⓘ.

Les écosystèmes numériques permettent de faciliter la gestion pédagogique, organisationnelle et administrative de la vie scolaire, de renforcer la communication entre les parents et l'école, de mieux rencontrer les besoins spécifiques de certains élèves…

Toutefois, les avantages du numérique s'accompagnent d'un risque croissant d'actes malveillants tels que des cyberattaques, du **rançonnement** ⓘ, de violation de la vie privée, etc.

En outre, les établissements scolaires possèdent de nombreuses informations sensibles relatives aux membres du personnel et surtout aux élèves, mineurs d'âge pour la plupart. Si les écoles ne prennent pas de mesures de sécurité suffisantes, elles peuvent devenir une cible de choix pour les malfaiteurs.

Les conséquences d'une cyberattaque peuvent être très lourdes pour une école : fuite de données sensibles, pertes de confiance des familles en l'institution scolaire, poursuites judiciaires, image de l'école écornée, perte financière, surcharge de travail pour récupérer des données perdues (données administratives, notes d'évaluations des élèves, préparations de leçons, etc.), et autres.

Élaboré dans le cadre du Pacte pour un Enseignement d'excellence, ce guide a pour vocation de soutenir les établissements scolaires dans le développement de leur écosystème numérique, en formulant des recommandations pour renforcer leur sécurité et la protection de leurs données. Les choix techniques pour la mise en œuvre relèvent quant à eux des établissements.

Les réalités des écoles étant très différentes (taille de l'établissement, niveau de développement de leur écosystème numérique, niveau de sécurité déjà mis en œuvre, délégué référent au numérique à disposition ou non, contrat éventuel avec une société spécialisée, etc.), les recommandations formulées dans ce guide se veulent d'ordre général. Chaque école pourra y puiser les mesures de sécurité qui correspondent le mieux à ses besoins, selon ses moyens et les risques auxquels elle fait face.

Aussi, dans le cadre de la transmission des données à l'Administration générale de l'Enseignement (AGE), à travers des applications telle que SIEL (Signalétique et inscription des élèves), l'AGE peut exiger des mesures spécifiques de sécurité encadrant l'utilisation de ses outils[1].

Dans le présent guide, pour chaque ensemble de recommandations, trois catégories de personnes sont ciblées : le responsable d'établissement, l'équipe éducative et enfin, le délégué référent au numérique (DRN) ou autre membre de la communauté éducative jouant un rôle de soutien à l'équipe éducative en matière de numérique[2].

Le vocabulaire utilisé dans le guide pour les deux premiers groupes se veut le plus accessible possible. Néanmoins, certaines mesures proposées aux responsables d'établissements peuvent nécessiter un certain degré de compétence technique et peuvent le cas échéant être mises en œuvre par d'autres personnes.

(1) Conformément à l'article 6 du décret du 25 avril 2019 relatif à la gouvernance numérique du système scolaire et à la transmission des données numériques dans l'enseignement obligatoire.
(2) Pour la suite du document, le terme employé est, par souci de concision, « délégué référent au numérique (DRN) ».

Les délégués référents au numérique (DRN) y trouveront quant à eux un vocabulaire et des mesures plus techniques pour leur permettre d'augmenter significativement le niveau de sécurité du système informatique de leur école. Enfin, la dernière partie du présent guide propose un glossaire pour expliciter certains termes techniques.

1.1 La sécurité du système informatique, pourquoi est-ce important ?

Voici quelques situations que de nombreuses écoles ont probablement déjà connues.

Mickaël, un adolescent de 16 ans, inscrit dans l'école de son quartier, a connu des problèmes avec la justice suite à des faits de violence. La police est en contact régulier avec l'école à ce sujet. Un hacker (pirate informatique) a réussi à intercepter les messages échangés entre l'école et la police au sujet de Mickaël. Il menace de les diffuser sur internet, à moins que l'école ne lui paye une rançon de plusieurs milliers d'euros.

Maryam est une fille de 7 ans. Elle connaît de sérieux problèmes de santé. Un membre du personnel a oublié de se déconnecter d'un ordinateur contenant des données personnelles, dont celles de Maryam. Un élève a pu prendre possession de ces données à partir de cet ordinateur. Il décide de publier sur internet toutes les données qu'il a subtilisées. Les parents de Maryam découvrent sur les réseaux sociaux que la vie privée de leur enfant s'y trouve exposée.

Un élève de l'école Y a réussi à pirater le système informatique de son établissement. Toutes les données importantes de l'école ont été supprimées : notes d'évaluations, rapports disciplinaires, absences des élèves et leurs justificatifs, plans individuels d'apprentissage (PIA)… Les membres du personnel ont dû consacrer des centaines d'heures à tenter de récupérer ces données et à les réencoder dans le système.

Comme l'indiquent ces quelques situations fictives et néanmoins réalistes, il y a un réel danger à voir des **données à caractère personnel (ou données personnelles)** ⓘ des élèves ou des membres de l'équipe éducative tomber entre de mauvaises mains.

D'une part, d'un point de vue éthique, l'école devrait pouvoir garantir la protection des données à caractère personnel des membres de son personnel et de ses élèves. En cas de perte ou de fuite de données, la confiance accordée aux écoles par les familles peut se détériorer, et l'image de l'école peut en pâtir sérieusement.

D'autre part, les établissements scolaires sont légalement responsables de la protection des données des élèves et des membres de leur personnel. En effet, le **Règlement général sur la protection des données (RGPD)** ⓘ impose aux organisations qui traitent des données à caractère personnel de prendre les mesures techniques et organisationnelles nécessaires à leur protection. Dès lors, une école qui ne sécuriserait pas ses données à caractère personnel pourrait s'exposer à des poursuites judiciaires.

Quelques chiffres sur les menaces de cybersécurité ⓘ pour l'école

Depuis que les écoles se sont engagées dans la transition numérique, le secteur éducatif est devenu l'une des principales cibles des hackers. Selon une étude réalisée par Sophos[1], en 2020 :

- sur 499 écoles interrogées dans le monde, 44% ont déclaré avoir été victimes de rançonnement par des hackers ;
- au total, les écoles ont dépensé 2,73 millions de dollars (2,41 millions d'euros) pour récupérer des données rançonnées par des hackers ;

Selon le NCSC (National Cyber Security Centre)[2], 83% des établissements scolaires au Royaume-Uni ont déclaré avoir subi un **incident de sécurité** ⓘ et 69% d'entre elles ont subi une attaque par **hameçonnage (phishing)** ⓘ.

(1) www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf
(2) www.nen.gov.uk/wp-content/uploads/2019/09/Cyber-Security-Schools-Audit-2019-NCSC-LGfL.pdf

1.2 La sécurité de l'information : quelques définitions

La sécurité de l'information

Il est important que les informations essentielles que détient un établissement scolaire restent **confidentielles** (seules les personnes autorisées doivent y avoir accès), **intègres** (il ne doit pas être possible de les altérer, volontairement ou non) et **disponibles** (lorsqu'elles sont sollicitées par une personne qui a le droit d'y accéder, par exemple par un parent d'élève).

Ces trois qualités : confidentialité, intégrité et disponibilité des données constituent le fondement de ce que l'on appelle « la sécurité de l'information ».

Quelle information sécuriser ?

L'école détient de nombreuses informations, dont certaines sont critiques et nécessitent un certain degré de protection. C'est le cas notamment des données à caractère personnel et des données confidentielles. Dans le présent guide, nous distinguons ces deux notions comme suit :

→ Les données à caractère personnel

Les **données à caractère personnel** ⓘ sont toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement[1]. Celles-ci peuvent revêtir un caractère « **sensibles** » ⓘ au sens du RGPD, et qui nécessitent une protection maximale :

- les certificats médicaux des élèves ou des messages des membres du personnel ;
- le relevé des absences ;
- les données relatives aux inscriptions et aux choix des cours des élèves (options, cours philosophiques, etc.)
- …

→ Les données confidentielles

Outre les données à caractère personnel, l'école détient de nombreuses informations importantes pour son bon fonctionnement et qui nécessitent d'être protégées, par exemple :

- l'état de ses comptes financiers ;
- ses prévisions budgétaires ;
- les plans des bâtiments ;
- les données d'ordre pédagogique ou organisationnel (bulletins, PIA, plans de pilotage…) ;
- …

(1) « Guide pratique : Comprendre et appliquer le RGPD en classe » du Service Général du Numérique éducatif de la FW-B : www.e-classe.be/resourcesingle/file/3802

2 SE CONSTITUER UN ÉCOSYSTÈME NUMÉRIQUE SÉCURISÉ

2.1 Qu'est-ce qu'un écosystème numérique ?

Dans la Stratégie numérique pour l'éducation de la FW-B adoptée dans le cadre du Pacte pour un Enseignement d'excellence[1], l'expression « écosystème numérique de l'école » est définie comme « un ensemble intégré de services numériques accessibles à la communauté éducative d'une école. Il permet à l'utilisateur d'accéder, selon son profil et son niveau d'habilitation, à des services et à des contenus numériques. Il offre un lieu d'échange et de collaboration entre les membres de l'équipe éducative, mais aussi avec les parents et les élèves.

Concrètement, les services offerts par les divers environnements numériques recouvrent de nombreux services utilisateurs de communication et de collaboration (courrier électronique, espaces d'échanges et de collaboration, affichage d'informations, publication web, conférence audio et vidéo), des services informationnels et documentaires (carnet d'adresses, agendas, accès aux ressources pédagogiques), des services d'accompagnement de l'élève (journal de classe, outils de suivi individuel des élèves, exercices de remédiation, affichage de l'emploi du temps), des services de production pédagogique et éducative ou encore des services utilitaires (réservation de salles et matériels, etc.).

Les écosystèmes numériques permettent également la numérisation d'un nombre croissant de procédures et d'échanges d'informations avec l'administration. »[2]

2.2 Quelques recommandations générales

→ Privilégier les outils proposés par l'administration et les FPO/PO qui s'assurent de répondre aux exigences de sécurité et de conformité à la législation.

→ En cas d'utilisation des services d'une société privée, rester vigilants vis-à-vis des fournisseurs de services, souvent gratuits, dont le modèle économique repose sur l'exploitation des données.

→ Dans la mesure où un établissement scolaire souhaite acquérir un outil pour développer son écosystème numérique, être attentif aux garanties qu'offrent les fournisseurs de service en matière de sécurité, et en particulier à la protection des données à caractère personnel telle qu'exigée par le RGPD.

La sécurité dépend autant de la vigilance des utilisateurs que de la configuration technique des outils. En effet, les risques en matière de fuite de données proviennent souvent d'erreurs humaines. Il incombe donc aux administrateurs et aux utilisateurs, quel que soit le niveau de sécurité des outils, d'adopter les mesures de précautions d'usage : gestion des mots de passe, gestion des accès et des permissions, etc.

(1) www.enseignement.be/index.php?page=28101
(2) Stratégie numérique pour l'éducation, p.44.

2.3 Quels critères de sécurité exiger auprès d'un prestataire externe ?

Une école souhaite se constituer un écosystème numérique. Pour ce faire, elle prospecte les solutions proposées par différents fournisseurs de service : quels critères retenir en matière de sécurité ?

Un fournisseur de service numérique devrait au minimum proposer :

- Par défaut, de ne récolter que les données personnelles qui sont strictement nécessaires au bon fonctionnement de ses services.
- Le stockage des **données personnelles et confidentielles** ⓘ dans un espace sécurisé à l'aide d'un chiffrement.
- L'hébergement des données personnelles sur un serveur situé en Europe. Dans le cas contraire, le fournisseur de services devrait offrir la possibilité de signer des modèles de contrats de transfert de données personnelles adoptés par la Commission européenne[1].
- Une seule authentification pour accéder à l'ensemble de ses services (SSO : Single Sign On). Cela permet de limiter le nombre de fois où l'utilisateur doit encoder son authentifiant et son mot de passe et par là même, cela réduit le risque de piratage de ses données d'identification.
- La **double authentification** ⓘ (par exemple : mot de passe + application sur smartphone), surtout pour l'accès à des comptes administrateurs ou d'autres comptes qui contiennent des données personnelles et/ou confidentielles.
- La possibilité de définir et paramétrer de manière précise les droits d'accès et les rôles (super administrateur / administrateur / utilisateur…), c'est-à-dire de proposer des accès différenciés en fonction des rôles et des fonctionnalités utilisées (par exemple : « gestion des PIA » uniquement accessible aux enseignants de l'élève concerné)…
- Prévoir l'obsolescence des accès (retirer les accès aux utilisateurs qui quittent l'établissement par exemple).
- La déconnexion d'un compte ouvert après une période d'inactivité de l'utilisateur. Idéalement, ce dernier doit pouvoir paramétrer lui-même la durée d'inactivité au-delà de laquelle l'outil doit se déconnecter automatiquement.
- Un refus temporaire d'accès au compte après plusieurs échecs de tentative de connexion. Par exemple : après X tentatives échouées, le compte reste inaccessible durant X minute(s) ainsi que le blocage du compte après un nombre déterminé d'échecs de connexion.
- L'exigence, lors de la création ou du renouvellement des données d'identification d'un compte, d'un mot de passe fort (comme un nombre suffisamment élevé et varié de caractères) et lui attribuer une durée de validité limitée.
- Le chiffrement de bout en bout des authentifiants, comme les mots de passe. Les données d'authentification ne doivent jamais être stockées « en clair » (elles doivent être chiffrées).
- Lorsque les services sont disponibles en ligne via une page web, ils doivent l'être à l'aide d'une connexion sécurisée (HTTPS).
- Le fournisseur dispose d'un helpdesk (support technique) en cas de piratage de son outil.

Notons par ailleurs que, conformément à l'art.28 du RGPD, une convention doit être rédigée lorsqu'une école recourt aux services d'une société externe qui implique un traitement de données à caractère personnel.

Le « Guide pratique : Comprendre et appliquer le RGPD en classe »[2] du Service général du Numérique éducatif fournit aux écoles des recommandations plus spécifiques sur les garanties que doit fournir un prestataire externe quand le service qu'il propose implique un traitement de données à caractère personnel.

(1) Les modèles de contrat se trouvent ici : eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=fr

(2) www.e-classe.be/resourcesingle/file/3802

3 CONSEILS PRATIQUES POUR SÉCURISER SON ÉCOSYSTÈME NUMÉRIQUE[1]

3.1 Sensibiliser les membres du personnel et les élèves

Pourquoi sensibiliser les utilisateurs ?

Sensibiliser les membres du personnel et les élèves aux bonnes pratiques en matière de sécurité est probablement l'une des mesures les plus importantes. En effet, la plupart des incidents en matière de sécurité informatique proviennent d'erreurs humaines.

De nombreuses personnes n'ont pas conscience du danger potentiel que représente une imprudence en matière de cybersécurité.

C'est pourquoi il est important de prévoir quelques actions de sensibilisation, pour s'assurer que les membres du personnel réduisent au maximum les risques de sécurité.

Sensibiliser : à quoi, et comment ?

Actions à entreprendre par la direction d'établissement[1]

Sensibiliser les membres du personnel

→ aux risques en matière de violation des données à caractère personnel

Vous pouvez rappeler aux membres du personnel les conséquences d'une violation de données à caractère personnel sur le plan éthique, financier, juridique… comme cité en introduction de ce guide.

→ au renforcement des mots de passe au sein de l'établissement

Les pirates informatiques peuvent assez facilement deviner un mot de passe ou le déterminer à l'aide d'un logiciel spécifique. C'est pourquoi il est essentiel de fournir aux utilisateurs des recommandations telles que mentionnées au **point 3.2 « Sécuriser les documents et les postes de travail »**

→ aux risques d'hameçonnage (phishing)

L'hameçonnage ou le phishing est une des techniques les plus fréquemment utilisées par les personnes malveillantes pour pirater un système informatique ou subtiliser des données[2]. Des recommandations sont formulées au **point 3.4 « Sécuriser les communications »** pour s'en prémunir au mieux. Il est important d'informer et sensibiliser régulièrement les utilisateurs pour se prémunir contre l'hameçonnage.

→ à l'utilisation d'outils respectueux du RGPD lorsque des données à caractère personnel sont manipulées

Le modèle économique de certaines entreprises repose essentiellement sur l'exploitation des données d'utilisateurs. C'est pourquoi il est essentiel de choisir les outils les plus respectueux possibles du RGPD. Lorsque le choix est limité, invitez les utilisateurs (enseignants, élèves…) à encoder le moins de données personnelles possible et à s'inscrire en usant d'un pseudo plutôt que de leur nom.

(1) Les recommandations pourvues du symbole sont considérées comme prioritaires.

(2) www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/arnaques-par-message-electronique-comment-identifier-et-dejouer-lhameconnage

→ aux réactions adéquates à adopter en cas de dysfonctionnement

Lorsque les utilisateurs (un enseignant par exemple) détectent un dysfonctionnement, ils doivent le signaler rapidement à leur direction (**voir le point 3.6 « Gérer les incidents ? »**).

→ à l'utilisation de moyens de stockages appropriés pour des données sensibles/confidentielles

Des données sensibles et/ou confidentielles devraient par exemple être prioritairement stockées sur un serveur ou un cloud sécurisé plutôt que sur une clé USB, à moins qu'elle ne soit cryptée. En effet, une clé USB peut se perdre facilement et pourrait tomber entre de mauvaises mains.

→ à l'importance de se déconnecter systématiquement d'un compte après utilisation

Cette règle est d'autant plus importante dans une école, dans la mesure où les ordinateurs sont souvent utilisés par différentes personnes (dans la salle des profs, dans une salle de classe, dans un local informatique…).

Sensibiliser à fréquence régulière

Idéalement, la sensibilisation doit avoir lieu régulièrement, au minimum une à deux fois par an.

Les campagnes de sensibilisation peuvent prendre différentes formes : via une note de services ou mail, lors de réunions de travail, de journées pédagogiques…

La check-list des mesures de sécurité proposées dans ce guide (**page 28**) peut servir de support à une campagne de sensibilisation.

Rédiger une charte d'utilisation responsable du numérique

Les éléments clés d'une charte pour l'équipe éducative sont présentés en annexe 2 à titre d'exemples. Vérifiez également auprès de votre FPO/PO s'il ne propose pas des documents de ce type.

Actions à entreprendre par l'équipe éducative

Sensibiliser les élèves à la cybersécurité

La sécurité informatique est un des champs d'apprentissage du référentiel de formation manuelle, technique, technologique et numérique (FMTTN) pour les élèves du tronc commun. Outre les contenus d'apprentissage du référentiel, la sensibilisation des élèves aux bonnes pratiques en matière de cybersécurité peut porter sur le renforcement des mots de passe, la gestion de leurs données personnelles, la prudence dans les usages des outils de communications et des réseaux sociaux…

Sensibiliser à fréquence régulière

La sensibilisation peut se faire à l'occasion d'un apprentissage au ou par le numérique, quel que soit la discipline enseignée et plus particulièrement dans le cadre de la formation manuelle, technique, technologique et numérique. Néanmoins, certaines dates clés peuvent servir de prétexte pour mener une campagne ciblée de sensibilisation à la cybersécurité comme le mois européen de la cybersécurité (ECSM) de l'Union européenne qui a lieu annuellement au mois d'octobre. Des plateformes en ligne de sensibilisation à destination des jeunes publics peuvent servir de support pour sensibiliser ses élèves : jedecide.be, safeonweb et les outils du Centre pour la Cybersécurité Belgique (**voir les références à la fin de ce guide**).

Participer avec son école à l'e-Safety Label

L'e-Safety Label est une initiative de l'European Schoolnet (réseau européen regroupant 33 ministères de l'éducation de l'UE). Cette initiative permet de s'inscrire dans une démarche d'échanges de bonnes pratiques en matière de cybersécurité, d'auto-évaluation et d'obtenir un label attestant du niveau de cybersécurité de son école[1].

Actions à entreprendre par le délégué référent au numérique

Aider la direction à cibler les actions de sensibilisation

Vous pouvez aider la direction d'établissement à orienter le contenu de la sensibilisation en fonction des besoins spécifiques de ce dernier. Par exemple, selon que l'école possède ou non un serveur, un fournisseur de services tel qu'un Environnement Numérique de Travail (ENT) ou un réseau Wi-Fi, la sensibilisation peut être orientée sur ce qu'il estime être des points prioritaires à améliorer.

Trouver un équilibre entre confort d'utilisation pour les membres du personnel et sécurité de l'information

Seules les données à caractère personnel et/ou confidentielles doivent faire l'objet d'une sécurisation maximale. L'expérience dans d'autres pays a montré que lorsque les contraintes de sécurité et/ou juridiques sont trop strictes, des enseignants se détournent des outils proposés par leur hiérarchie au profit d'outils moins sécurisés, mais plus efficaces et plus faciles d'utilisation. Un équilibre est à trouver pour ne pas rendre l'accès aux outils sécurisés trop contraignant pour les membres du personnel, sans pour autant transiger sur la sécurité des données à caractère personnel.

Contribuer à l'élaboration ou l'adaptation d'une charte d'utilisation responsable du numérique

Vous pouvez contribuer à rédiger la charte relative à l'utilisation du numérique. Les recommandations inscrites dans ce guide, ainsi que la check-list (**page 28**), peuvent servir à alimenter cette charte (**voir l'annexe 2**).

(1) www.esafetylabel.eu/home

3.2 Sécuriser les documents et les postes de travail

Pourquoi sécuriser les documents et les postes de travail ?

Les établissements scolaires accueillent de nombreuses personnes : des membres du personnel, des élèves, mais aussi des parents d'élèves ainsi que des personnes extérieures (sociétés externes, visiteurs…). Par ailleurs, les établissements scolaires ne sont pas toujours à l'abri d'une intrusion illégitime dans leurs bâtiments.

- Une personne malveillante peut prendre possession d'un poste de travail (ordinateur, tablette, imprimante…) et, en quelques secondes à peine, subtiliser des données confidentielles, installer un logiciel espion, infecter tout le réseau de l'établissement, et plus encore.
- Il en est de même des documents en format papier : il est facile de les subtiliser, d'en lire rapidement le contenu, d'en prendre une photo, etc.
- Enfin, le matériel informatique et les documents ne sont pas toujours suffisamment protégés contre un incident environnemental (incendie, dégât des eaux, etc.) qui détruirait les données utiles au bon fonctionnement de l'école.

Il est donc nécessaire d'une part, d'assurer la sécurité du matériel informatique contre d'éventuels vols, attaques ou accidents et d'autre part, de sécuriser les documents en format papier qui contiennent des données à caractère personnel et/ou confidentielles.

Comment sécuriser les documents et les postes de travail ?

Actions à entreprendre par la direction d'établissement

Sécuriser les locaux sensibles

Cette mesure concerne les locaux où se trouvent des données à caractère personnel et/ou confidentielles : bureau du secrétariat, de la direction, de l'économat, des éducateurs, du CPMS, local informatique, local du serveur… Outre le verrou des portes de ces locaux, il est utile d'installer des alarmes anti-intrusion dans les locaux sensibles et de les vérifier régulièrement.

Définir les droits d'accès, les rôles et leur obsolescence

L'accès à certaines fonctionnalités et à certaines données, les rôles attribués aux différents utilisateurs, doivent être soigneusement paramétrés.

Certains « privilèges » dans l'utilisation des outils numériques doivent être réservés aux détenteurs du rôle d'administrateur. Les utilisateurs quant à eux n'ont accès qu'aux fonctionnalités qui leur sont utiles et qui ne comportent pas de risque en matière de sécurité. L'installation de logiciels par exemple devrait être réservée aux administrateurs, de sorte à réduire le risque d'installation involontaire d'un logiciel malveillant.

Enfin, prévoyez l'obsolescence des accès et/ou la modification des rôles notamment lorsque les utilisateurs changent de fonction ou quittent l'établissement.

Veiller à la mise à jour régulière du système d'exploitation des postes de travail

Le système d'exploitation (Linux, Mac OS, Windows, iOS, Android…) intégré aux terminaux (ordinateurs, tablettes…) doit être régulièrement mis à jour. En effet, les mises à jour contiennent souvent des correctifs prévus pour renforcer la sécurité.

Équiper les postes de travail (ordinateurs, tablettes…) d'un antivirus de qualité

Des comparatifs sont disponibles sur internet. Ils permettent de choisir un antivirus dont la qualité a été testée. Veillez également à mettre à jour l'antivirus régulièrement. Les licences des antivirus doivent être régulièrement renouvelées.

Limiter l'accès au serveur ?

Si l'école possède un serveur, il est important de l'installer dans un local sécurisé et fermé à clé. Un nombre limité d'individus doit pouvoir avoir accès au local.

Sécuriser les documents (papier) contenant des données à caractère personnel et/ou confidentielles

Les documents sensibles devraient être placés dans une armoire fermée à clé. Lorsqu'ils sont jetés, ils devraient être détruits à l'aide d'une déchiqueteuse. Vous pouvez également numériser les documents papiers pour les centraliser et assurer leur sauvegarde dans un environnement sécurisé au cas où, notamment, vous devriez produire des documents pour un tiers[1].

Veiller à la sécurité des imprimantes

Les imprimantes connectées au réseau voient transiter quotidiennement de nombreux documents confidentiels. Lors d'un achat, il est recommandé de choisir des imprimantes sécurisées dès la conception (« by design »). Par exemple, l'imprimante peut :

- être configurée pour supprimer automatiquement de son disque dur les données une fois imprimées ;
- chiffrer les données qu'elle reçoit et imprime ;
- permettre le contrôle des accès utilisateurs ;
- posséder un système de protection des ports (USB par exemple) ;
- permettre de restreindre certaines fonctionnalités à différentes catégories d'utilisateurs…

(1) Pour identifier les informations que l'on peut communiquer à un tiers, en plus du RGPD, se référer à la législation en la matière disponible sur cada.cfwb.be

Lors d'un achat, demandez au fournisseur si l'imprimante qu'il propose est sécurisée et si oui, comment la paramétrer au mieux. Pour vos imprimantes existantes, vous pouvez vérifier si des fonctionnalités de sécurité sont présentes et les activer le cas échéant.

Actions à entreprendre par la direction et l'équipe éducative

Renforcer les mots de passe

- Utilisez exclusivement la **double authentification** ? pour les comptes administrateurs (exemple : mot de passe + téléphone), ainsi que pour ceux qui donnent accès à des données personnelles et/ou confidentielles.
- Utilisez de préférence la double authentification pour les comptes utilisateurs dans les autres cas.
- Adoptez un mot de passe complexe contenant un maximum de caractères, combinant lettres minuscules et majuscules, chiffres et caractères spéciaux (tels que « » +/-*%^$ et autres).
- Adoptez un mot de passe différent pour chacun des comptes en ligne.
- Utilisez un gestionnaire de mot de passe (ex. : Keepass, Zenway, Passwordsafe…). Celui-ci peut vous aider à sauvegarder vos différents mots de passe de manière sécurisée et/ou générer des mots de passe forts.

Voir le **point 6. « En savoir plus »** pour plus d'informations au sujet l'utilisation des mots de passe.

Verrouiller sa session dès que l'on quitte son poste de travail

Même si vous devez quitter votre appareil un court instant, veillez à verrouiller votre session pour éviter une intrusion furtive. Il suffit de quelques secondes pour infecter un appareil.

Les raccourcis suivants vous permet de le faire rapidement : sur Linux, « Ctrl » + « Alt » + « L » ; sur Windows, « touche Windows » + « L » ; sur Mac, « Contrôle » + « Commande » + « Q » ; sur Chromebook, « Lanceur d'applications » + « L ».

Distinguer l'usage du matériel privé et professionnel

Dans la mesure du possible, utiliser le matériel professionnel (l'ordinateur de l'école) lorsqu'il s'agit de manipuler des données à caractère personnel ou confidentielles (le dossier disciplinaire d'un élève par exemple) et réserver l'usage du matériel personnel aux autres données (préparation de cours par exemple).

Veiller à ne pas laisser de documents contenant des données à caractère personnel/ confidentielles dans l'imprimante

Il peut arriver à tout le monde d'oublier de récupérer un document dans l'imprimante. Or, un document imprimé peut très bien contenir des données à caractère personnel ou confidentielles. Il est donc recommandé de :

- récupérer tous les documents aussitôt l'impression terminée ;
- vérifier régulièrement qu'aucun document ne réside dans l'imprimante après une copie ou un scan.

Actions à entreprendre par le délégué référent au numérique

Programmer le verrouillage automatique de session

Par exemple, une durée de 5 à 15 minutes, à discuter avec vos collègues utilisateurs.

Conseiller la direction d'établissement sur le choix de l'antivirus à adopter

L'antivirus peut être mis à l'épreuve à l'aide du test EICAR. Il s'agit d'un fichier informatique développé par l'European Institute for Computer Antivirus Research pour tester la réponse d'un antivirus sans utiliser de réels virus qui pourraient endommager les postes de travail.

Installer un « pare-feu » (firewall) ?

Les postes de travail et les serveurs ayant une connexion directe à internet doivent être équipés d'un pare-feu basé sur l'hôte (ordinateur ou périphérique connecté au réseau).

Réaliser les mises à jour et correctifs de sécurité

Mettre à jour les systèmes d'exploitation, les applications, logiciels de bureautique, lecteurs de fichiers (PDF par exemple), navigateurs, plug-ins…

Recueillir l'accord de l'utilisateur avant toute intervention sur son poste

Cela permet d'éviter les malentendus et d'apaiser les craintes de certains utilisateurs quant à la sauvegarde de leurs données.

Adopter une stratégie pour les clés usb

Les clés usb peuvent contenir des données qui nécessitent une protection, et peuvent facilement se perdre ou être subtilisées.
C'est pourquoi vous vous pouvez, par exemple, adopter une ou plusieurs de ces mesures :

- empêcher purement et simplement l'utilisation des clés USB ;
- ne l'autoriser que sur certains postes via une gestion centralisée ;
- l'autoriser et avoir des antivirus qui scannent automatiquement.

3.3 Sécuriser le stockage des données

Pourquoi sécuriser le stockage des données ?

La perte de données peut générer une charge de travail extrêmement importante et très chronophage. En effet, qu'il s'agisse de préparation de leçons, de données administratives, de comptabilité… Si ces données sont perdues, ce sont de nombreuses et précieuses heures de travail qu'il faudra consacrer pour les reproduire.

La perte de données sensibles (une donnée de santé, l'orientation philosophique d'un élève, d'un membre du personnel…) peut s'avérer encore plus problématique. En effet, si ces données sont rendues publiques, involontairement ou de manière délibérée et malveillante, les conséquences peuvent être dommageables pour la victime. En outre, l'école s'expose à des poursuites judiciaires et devra alors établir qu'elle a pris les mesures de sécurité nécessaires pour protéger ces données, comme l'exige l'article 32 du RGPD[1].

Comment stocker ses données de manière sécurisée ?

Actions à entreprendre par la direction d'établissement

Sauvegarder les données importantes régulièrement

Pour se préserver des conséquences d'une perte de données, il est essentiel de les sauvegarder régulièrement. Outre l'obligation légale de protéger et de conserver certaines données, la sauvegarde des informations vous fait économiser un temps précieux si vous perdez des données essentielles au bon fonctionnement de l'établissement et au travail en classe des enseignants.

Chiffrer les données stockées

Si les données sont stockées sur un disque dur, veillez à chiffrer les données. Ainsi, si le disque dur venait à disparaitre, personne n'aurait accès aux données qui s'y trouvent (**Voir le point 6. « En savoir plus »** de ce document pour savoir comment chiffrer des documents).

Le chiffrement des données est également utile dans un espace de stockage en ligne (cloud). En effet, cela vous garantira que, ni le fournisseur du service cloud, ni personne d'autre ne pourra lire et exploiter vos données.

Sauvegarder ses données dans différents espaces de stockage physiques ou en ligne (cloud)

Les données doivent idéalement être sauvegardées sur plusieurs supports sécurisés. Ainsi, si les données sont perdues dans un espace de stockage, elles peuvent être aisément récupérées dans un autre.

Délocaliser le support physique de sauvegarde

Il est conseillé de prévoir un lieu de stockage supplémentaire, dans un bâtiment différent par exemple, ou en ligne sur un cloud (espace de stockage en ligne) sécurisé.

(1) « … le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque… » art.32 du RGPD.

Sécuriser les comptes du serveur

Les mots de passe par défaut livrés avec le serveur doivent être modifiés et remplacés par des mots de passe forts, les comptes non utilisés doivent être désactivés et le nombre d'administrateurs doit être limité au strict nécessaire.

Actions à entreprendre par la direction et l'équipe éducative

Privilégier un espace de stockage en ligne (cloud) sécurisé et localisé en Europe

Si vous utilisez un espace de stockage en ligne, il est important de vous assurer que l'espace est sécurisé, par exemple en s'assurant qu'il soit certifié **ISO 27001** ⓘ (norme internationale de sécurité des systèmes d'information).

Privilégier les clés USB chiffrées

Les clés USB peuvent facilement se perdre et tomber entre les mains d'une personne malveillante. Si vous devez stocker des données confidentielles et/ou à caractère personnel, privilégiez une clé USB cryptée. Le contenu de celle-ci ne sera alors accessible qu'après avoir utilisé un code ou une donnée biométrique (empreinte par exemple).

Aussi, ne branchez sur votre ordinateur que votre clé USB personnelle ou celle d'une personne de confiance. Une clé USB peut contenir un logiciel malveillant indétectable par votre ordinateur et l'infecter aisément.

Actions à entreprendre par le délégué référent au numérique

Éviter la connexion directe à distance aux serveurs

Utilisez un **VPN** ?, un mot de passe et vérifiez les logs d'accès (registre qui contient de nombreuses informations, dont les requêtes faites au serveur par des utilisateurs).

Changer les mots de passe par défaut et désactiver les comptes non utilisés

C'est notamment le cas du mot de passe par défaut fourni avec le serveur par exemple. Veillez à supprimer les comptes non utilisés, car ils sont les plus vulnérables au piratage.

Stocker les sauvegardes dans un coffre-fort ou dans un centre de données sécurisé

Par exemple, un cloud certifié ISO 27001.

Chiffrer les données à caractère personnel et/ou confidentielles stockées dans le cloud

Certaines solutions de cloud permettent de chiffrer les données avec une clé côté client avant transfert, ce qui rend impossible l'exploitation des données pour le fournisseur, et répond par ailleurs aux exigences du RGPD.

Verrouiller automatiquement les postes de travail et les appareils mobiles non utilisés

Prévoyez un délai d'inactivité assez court après lequel le poste de travail se verrouille automatiquement.

Stocker ou copier toutes les données via un service de stockage

Plusieurs solutions de stockage peuvent être envisagées: serveurs, NAS (Network Area Storage) ou un service cloud.

Chiffrer les messages électroniques qui contiennent des données sensibles ou confidentielles

Vous trouverez des conseils pratiques relatifs au chiffrement sur le site de la Commission nationale de l'informatique et des libertés (France) en suivant ce lien :

› **www.cnil.fr/fr/securite-securiser-les-echanges-avec-dautres-organismes**

3.4 Sécuriser les communications

Pourquoi sécuriser les communications ?

Des personnes malveillantes pourraient prendre possession, et rendre publiques, des informations échangées par email (ou autres outils de communication : Whatsapp, Messenger, Signal…) entre les membres du personnel, avec les élèves, les parents ou d'autres partenaires tels que la police, le CPMS, etc.

Les outils de communication constituent une des principales portes d'entrée des pirates informatiques. En effet, ces outils centralisent de nombreuses données confidentielles et souvent de très nombreuses données à caractère personnel.

En prenant possession d'une messagerie, une personne malveillante peut manipuler les messages de sa victime, envoyer de faux messages aux contacts de cette dernière et les piéger à leur tour, infecter leurs machines, les escroquer…

Comment sécuriser ses communications ?

Actions à entreprendre par la direction d'établissement

Utiliser une adresse email professionnelle pour les échanges dans le cadre scolaire

Utiliser une boite personnelle à des fins professionnelles est un risque important pour l'établissement. Dans ce cas, les données sortent du contexte professionnel et ne sont plus sous le contrôle de l'établissement. Cela peut également poser problème lorsqu'un des utilisateurs quitte l'école en étant en possession de certaines informations, et éventuellement conduire à des dérives.

Éviter de partager une boite email avec d'autres personnes

Une adresse email ou une boite email est personnelle et ne doit jamais être partagée. Hormis les adresses génériques de type « info@ecole.be » (exemple), une boite email ne doit être accessible qu'aux personnes habilitées à prendre en charge les messages. Si vous devez permettre l'accès à vos messages à une tierce personne (un remplaçant par exemple), activez plutôt le « transfert automatique des messages » sur votre boite email. Vos emails lui seront alors automatiquement transférés.

Utiliser un nom de domaine au nom de l'établissement

Si les directions d'établissements possèdent une adresse email professionnelle fournie par Fédération Wallonie-Bruxelles, il n'en est pas de même pour les autres membres du personnel. Il est donc utile de réserver un nom de domaine propre à l'école auprès d'un prestataire de service (hébergeur ou agent d'enregistrement) et de créer corollairement des adresses email au nom de l'école (par exemple : l'École de Châtelet loue auprès d'un hébergeur le nom de domaine ecoledechatelet.be. Elle crée ensuite des adresses email pour son équipe éducative de type nom.prenom@ecole-dechatelet.be).

Le nom de domaine (par exemple : @ecole-untel.be) renforce la confiance dans l'identité de l'établissement. Il permet au récepteur du message de s'assurer que l'adresse appartient bien à l'école, ce que ne permettent pas les adresses email gratuites (de type ecole-untel@hotmail.be, ecole-untel@gmail.com, ecole-untel@yahoo.be…).

Ce dernier type d'adresses email sont par ailleurs souvent utilisées par des personnes malveillantes pour piéger leurs victimes en se faisant passer pour une institution reconnue.

Organiser la gestion des boites email et autres outils de communication (départs, suspensions…)

Si un membre du personnel quitte l'établissement, il est nécessaire de suspendre sa boite email (et autres outils de communication). Une boite email active et/ou délaissée représente un risque important pour l'établissement, car elle contient encore des données à caractère personnel et/ou confidentielles et elle pourrait en outre être détournée.

Privilégier les outils de communication dont le prestataire est européen

Le RGPD favorise l'adoption d'hébergements de données situés géographiquement en Europe. Étant donné la criticité des données, soyez attentif à la solution choisie et aux garanties données en termes de conformité au RGPD par le prestataire. Il est par ailleurs vivement conseillé d'opter pour un prestataire européen.

Actions à entreprendre par la direction et l'équipe éducative

Se protéger des messages de phishing (hameçonnage)

Un message de phishing est souvent reconnaissable par un ou plusieurs des indices suivants :

- l'adresse email de l'expéditeur est inconnue, ou non officielle : par ex. un message censé provenir de la police et dont l'adresse email se termine par @gmail.com ;
- le message appelle à une réaction rapide et urgente ;
- le message est inattendu : par ex. il fait référence à un achat que vous n'avez jamais effectué ;
- il vous demande de communiquer des données personnelles ;
- il vous demande d'ouvrir un fichier en pièce jointe ;
- il vous demande de cliquer sur un lien ;
- il contient des fautes de langue, mais ce n'est pas toujours le cas.

Si vous recevez un message de phishing :

- transférez-le à **suspect@safeonweb.be**
- ne le transférez à aucun de vos contacts ;
- évitez d'ouvrir les fichiers en pièce jointe, de cliquer sur un lien, de répondre au mail… ;
- vous pouvez aussi prendre directement contact avec l'organisation dont prétend provenir le message pour vérifier son authenticité ou simplement leur signaler la fraude.

Si malgré vos précautions, vous avez été victime d'une fraude au phishing :

- changez les mots de passe de votre messagerie et des comptes qui y sont liés ;
- portez plainte à la police et/ou contactez votre banque, le cas échéant ;
- prévenez vos contacts si un message leur a été envoyé depuis votre compte.

Vous trouverez des informations détaillées sur le phishing dans le **point 6. « En savoir plus »**.

Choisir un outil de communication en fonction du contenu du message

Cette recommandation vaut spécifiquement pour les messages qui revêtent un caractère sensible ou confidentiel. Dans ce cas particulier, il est préférable de privilégier une autre voie de communication que les messageries non professionnelles.

Sécuriser l'accès à son service de messagerie

Il est conseillé d'utiliser un mot de passe fort, connu de vous seul et qui n'est pas utilisé pour un autre service web. La double authentification reste par ailleurs une meilleure protection que la simple utilisation d'un mot de passe. Vous pouvez vous référer aux recommandations en matière de mot de passe dans le **point 3.1 « Sensibiliser les membres du personnel et les élèves » à « Actions à entreprendre par la direction d'établissement ».**

Supprimer les messages après leur traitement

Les emails et autres messages sont souvent utilisés comme un espace où l'on sauvegarde des informations et/ou des fichiers reçus. Or, il est plus prudent de télécharger ces données et de les sauvegarder sur un espace de stockage physique ou virtuel sécurisé, et d'ensuite supprimer ces messages (en particulier ceux qui contiennent des données confidentielles ou à caractère personnel). Cela réduit le risque de fuite ou de perte de données en cas d'intrusion dans votre messagerie.

Actions à entreprendre par l'équipe éducative

Privilégier les communications via la plateforme numérique de l'école lorsqu'elle existe

Les risques de fuite de données devraient être réduits si vous utilisez la plateforme sécurisée de votre établissement plutôt qu'un outil grand public.

Informer la direction d'établissement lorsqu'un outil non fourni par l'école est utilisé

Cela permettra au chef d'établissement d'avoir un aperçu des outils utilisés au sein de son établissement et de prévenir les risques éventuels.

Lorsque ces outils servent aux échanges avec les élèves, une autorisation préalable des parents, des personnes investies de l'autorité parentale ou de l'élève majeur, est requise.

Privilégier les outils qui respectent le mieux la vie privée

Une recherche rapide sur internet peut vous donner un aperçu du niveau de sécurité de l'outil qui vous intéresse. Vous pouvez par exemple vérifier les points suivants : les messages sont chiffrés, l'outil collecte le moins possible de données à caractère personnel (numéro de téléphone, adresse email, nom et prénom, etc. notamment lors de l'inscription), il se conforme mieux qu'un autre outil au RGPD…

Éviter de partager sa boite email avec un collègue

De même que, spontanément, vous ne partagez pas votre boite email privée avec vos collègues, il est important de ne pas donner accès à votre boite email professionnelle. En effet, les emails contiennent souvent des données à caractère personnel, sensibles et/ou confidentielles.

Se déconnecter de sa boite email après utilisation sur un ordinateur partagé

Un ordinateur partagé est une source de risque important. Si vous vous connectez à votre boite email personnelle ou professionnelle ou à tout autre service de communication, pensez toujours à bien fermer votre session.

Activer le chiffrement des messages lorsqu'il ne l'est pas par défaut

Certaines applications prévoient le chiffrement des messages sans toutefois le paramétrer par défaut, il faut donc l'activer soi-même.

Paramétrer les outils de visioconférence

Par exemple : n'acceptez que les personnes invitées (activez la fonction « salle d'attente », mot de passe d'entrée à la salle virtuelle), empêchez l'enregistrement de la réunion, limitez ou empêchez les échanges écrits à travers le « chat », empêchez la poursuite de la réunion par les utilisateurs après le départ de l'organisateur…

Actions à entreprendre par le délégué référent au numérique

Imposer la double authentification aux comptes sensibles

Tous les services de messagerie professionnelle proposent aujourd'hui une authentification renforcée. Aujourd'hui indispensable, cette mesure devrait être encouragée au maximum et rendue obligatoire dans certains cas, comme pour les comptes administrateurs par exemple.

Recourir à une gestion centralisée des différentes adresses email

Il est important de reposer sur une infrastructure centralisant la gestion des boites email avec des politiques spécifiques de gestion : politique des mots de passe, conditions d'accès, gestion des nouveaux et anciens comptes, archivage, etc.

Restreindre l'accès géographique et activer les notifications d'alertes pour les nouvelles connexions

Il est conseillé de mettre en œuvre certaines protections comme la restriction géographique en ce qui concerne la connexion ou encore la confirmation de nouvelles connexions à partir de nouveaux ordinateurs, smartphones ou navigateurs.

Sensibiliser les utilisateurs aux emails malveillants

Une séance de sensibilisation récurrente aux bonnes pratiques est importante et nécessaire. Les outils mis à disposition au sein de l'école et les politiques de sécurité doivent être expliqués aux utilisateurs et aux responsables de l'établissement.

3.5 Sécuriser son réseau Wi-Fi

Pourquoi sécuriser le Wi-Fi ?

Si le réseau Wi-Fi n'est pas sécurisé, une personne malveillante peut intercepter les données qui y circulent afin de les voler, les détruire ou encore demander une rançon.

Une personne malveillante pourrait également se connecter à internet au moyen du réseau de l'école pour mener des attaques sur d'autres personnes ou organisations. Si cette attaque provenait du réseau de l'école, cette dernière pourrait être tenue pour responsable de l'acte malveillant.

Enfin, il est possible de mener une intrusion dans le réseau d'un établissement dans le but de le rendre inopérant et perturber ainsi le bon fonctionnement du système informatique de l'école.

Comment sécuriser son réseau Wi-Fi ?

Actions à entreprendre par la direction d'établissement

Vérifier que le réseau Wi-Fi est sécurisé

Vérifiez que le chiffrement **WPA2** ou **WPA3** ⓘ est activé sur le routeur, et activez-le si ce n'est pas le cas. Demandez l'aide de votre fournisseur d'accès à internet si personne au sein de votre établissement n'a les compétences techniques pour le faire.

Changer les mots de passe par défaut associés aux appareils connectés au réseau

Mettez régulièrement à jour vos appareils connectés à votre réseau (routeurs, photocopieuses, imprimantes, amplificateurs de réseau…), et changez les mots de passe par défaut qui leur sont associés.

Choisir un mot de passe complexe pour votre réseau Wi-Fi

Voir les recommandations en matière de mot de passe dans le **point 3.1 «Sensibiliser les membres du personnel et les élèves» à «Actions à entreprendre par la direction d'établissement».**

Dissocier le réseau Wi-Fi des membres du personnel administratif, éducatif, élèves et invités

Demandez au responsable technique (une société privée, votre référent numérique…) de créer des réseaux différents pour le personnel administratif, le personnel éducatif, les élèves et éventuellement pour les personnes extérieures à l'établissement (membres du PO, syndicats, association de parents, animateurs pédagogiques, CPMS, etc.).

Actions à entreprendre par l'équipe éducative

Garder secret le mot de passe du réseau Wi-Fi

Si le réseau Wi-Fi des membres du personnel est différent de celui des élèves et des visiteurs, il est impératif de ne jamais leur divulguer le mot de passe.

Se connecter à un réseau privé et de confiance plutôt qu'à un réseau public (Hotspot) lorsqu'on est en déplacement

Les réseaux Wi-Fi publics (exemple : Wi-Fi des centres commerciaux, des restaurants, cafés, etc.) sont souvent peu ou pas sécurisés. Ils peuvent également avoir été créés par des pirates en vue de vous subtiliser des données ou corrompre votre machine.

En l'absence d'un réseau wifi fiable, utilisez de préférence la connexion partagée du réseau 4G par l'intermédiaire d'un smartphone.

Actions à entreprendre par le délégué référent au numérique

Sécuriser correctement le réseau Wi-Fi

Assurez-vous que le chiffrement n'est pas en **WEP**, mais en **WPA2** (?) au minimum et que le mot de passe associé soit complexe.

Identifier le matériel à connecter au réseau

Utilisez les identifiants des cartes réseau (adresses MAC) afin d'interdire la connexion d'un dispositif non répertorié.

Proposer un VPN pour l'accès à distance

Pour que les membres du personnel puissent se connecter au réseau de l'établissement à distance, il est plus sûr de proposer une solution VPN.

S'assurer qu'aucune interface d'administration n'est accessible directement depuis internet

L'accès au système par l'administrateur, notamment pour la maintenance, doit se faire via un VPN.

Limiter les accès internet

Bloquez les services non nécessaires tels que le VoIP, le « pair à pair »…

Limiter les flux réseau au strict nécessaire

Filtrer les flux entrants et sortants sur les équipements (pare-feu, proxy, serveurs…). « Par exemple, si un serveur web utilise obligatoirement HTTPS, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports[1] » (Commission nationale de l'informatique et des libertés - France).

Cloisonner le réseau

Distinguez un réseau interne sur lequel aucune connexion venant d'internet n'est autorisée, et un réseau DMZ (DeMilitarized Zone) accessible depuis internet, en les séparant par des passerelles (pare-feux).

Recourir à un système de détection d'intrusion (IDS)

Ces systèmes permettent d'analyser le trafic réseau pour détecter d'éventuelles attaques. Pensez à avertir les utilisateurs si leurs contenus doivent être analysés.

(1) www.cnil.fr/fr/securite-proteger-le-reseau-informatique-interne

3.6 Gérer les incidents

Pourquoi prévoir un plan de gestion des incidents ?

Quel que soit le niveau de sécurité mis en œuvre au sein d'un établissement, un incident ou une cyberattaque n'est jamais à exclure. En effet, un incident peut aussi bien provenir d'une simple erreur humaine que d'une cyberattaque très sophistiquée menée par des experts en la matière. Il est donc prudent de prévoir la réaction à adopter en cas d'incident.

Qu'est-ce qu'un incident ?

Un incident de sécurité est un événement constituant un risque sérieux pour l'école et qui peut perturber son bon fonctionnement. Celui-ci peut se matérialiser, entre autres, par :

- une cyberattaque visant par exemple à rendre le système informatique inopérable, à subtiliser des données confidentielles, accéder de manière illégitime à des données confidentielles, etc. ;
- une erreur ou un usage inapproprié (involontaire ou non) des outils informatiques, par exemple un utilisateur laissant son compte ouvert sur son ordinateur en son absence, donnant un accès involontaire à ses emails ou fichiers confidentiels ;
- un incident technique ou lié à un sinistre : panne d'électricité, incendie, dégât des eaux… ;
- un vol de matériel au sein de l'établissement ;
- …

Comment gérer un incident ?

Actions à entreprendre par la direction d'établissement

Définir une procédure en cas d'incident et la communiquer aux membres du personnel

Informez les membres du personnel des réactions à adopter en cas d'incident, telles que contacter immédiatement la direction d'établissement, ne pas essayer de résoudre le problème soi-même, réagir adéquatement à la réception d'un email frauduleux…

Prévoir une liste de personnes à contacter en cas d'incident

Par exemple :

- en cas de cyberattaque : portez plainte auprès de la police locale, faites éventuellement appel à une société spécialisée ou à la **Computer Emergency Response Team (CERT)**[1] ⍰ qui vous donnera les premiers conseils à suivre… ;
- en cas de fuite de données, votre délégué à la protection des données, le responsable de traitement de vos données (l'AGE par exemple) et l'**APD (Autorité de Protection des Données)** ⍰. Dans certains cas, lorsqu'il y a un risque de préjudice important lié à la perte de données personnelles, une notification doit être faite auprès de l'APD dans les 72h[2] ;
- au cas où des coordonnées bancaires ont été communiquées : contactez votre banque et/ou cardstop au 078 170 170 ;
- envisagez les personnes à contacter en cas de perte des données liées à une dégradation du matériel, à un vol de matériel, à un incendie, etc.

Conservez cette liste dans un format papier (pour qu'elle soit disponible au moment où le système informatique est inaccessible).

(1) www.cert.be/fr/signaler-un-incident

(2) Le signalement doit se faire sur le formulaire suivant : www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles

Réagir rapidement à une attaque

Plus la réaction est rapide, plus les chances d'arrêter une attaque sont grandes. Il est donc essentiel de réagir rapidement pour prendre les mesures techniques nécessaires afin de limiter l'impact d'une attaque. La CERT pourra vous donner des conseils ciblés en fonction de l'incident rencontré.

Contacter le fournisseur de service concerné

Si l'école dispose d'une plateforme numérique, d'un logiciel pédagogique ou administratif, il est nécessaire d'avertir le plus rapidement possible le fournisseur de service pour qu'il prenne les mesures utiles.

Comprendre l'incident et enregistrer les preuves

Bien qu'il faille agir rapidement, il est nécessaire de prendre le temps d'analyser l'incident (avec l'aide d'une personne qualifiée, une société spécialisée, la police…) pour comprendre comment elle a pu se réaliser. Il s'agit également d'enregistrer un maximum de preuves pour permettre à la police et à la justice de faire leur travail.

Anticiper le fait que les cyberattaques se déroulent en général en dehors des heures de bureau, et pourraient avoir lieu durant les vacances scolaires

La plupart du temps, les attaques se déroulent volontairement en dehors des horaires scolaires.

Demander aux membres du personnel de signaler immédiatement les incidents à la direction

Les dysfonctionnements sont souvent repérés par les utilisateurs. Assurez-vous qu'ils sachent qui contacter (le chef d'établissement, éventuellement le référent numérique…) et quand.

Par exemple : lorsqu'une fuite de données personnelles doit être signalée à l'APD, la notification doit se faire dans les 72 heures. Il est donc nécessaire de prévoir un processus de signalement rapide au sein de l'établissement scolaire.

Les déclarations d'incidents doivent être encouragées. Il est donc nécessaire de ne pas sanctionner les maladresses, à moins qu'elles n'aient été commises de manière délibérée. Il s'agit d'éviter que des incidents soient passés sous silence.

Prévoir un message d'alerte aux différentes cibles

Membres du personnel, élèves, parents, administration… Un exemple de message d'alerte est présent en **annexe 1** de cette publication.

Prévoir un backup (?) (sauvegarde de données) actualisé et exploitable

Si vous disposez d'un backup suffisamment sécurisé pour être épargné par un incident (par exemple, localisé dans un endroit différent), il vous permettra de reprendre vos activités rapidement et diminuera votre charge de travail de manière conséquente.
Voir le point 3.3 « Sécuriser le stockage des données » pour plus de détails sur la manière de sauvegarder ses données.

Enregistrer les preuves pour les présenter à la justice le cas échéant

Une preuve peut par exemple se matérialiser par : un journal de connexions, un ou des message(s) reçu(s), une trace d'intrusion dans un local sensible…

Refuser de payer une rançon

Dans le cas où une personne malveillante subtilise des données et exige une rançon pour vous les restituer, répondre à cette demande est une très mauvaise idée. En effet, rien ne garantit que cette personne restituera les données après paiement de la rançon. De plus, cela ne ferait que renforcer cette forme de criminalité.

Envisager l'opportunité de souscrire à une assurance pour se couvrir contre les cyberattaques

Une assurance peut, entre autres, vous assister en cas de cyberattaque, intervenir dans les frais de remise en état de votre système informatique et dans les frais liés à la protection de la réputation de votre établissement, etc.

Actions à entreprendre par l'équipe éducative

Avertir immédiatement la direction de l'établissement en cas d'incident

Il est important de le faire rapidement (y compris en dehors horaires scolaires si possible) pour permettre à la direction de l'établissement de prendre les mesures nécessaires afin de limiter au maximum les impacts d'un incident ou d'une cyberattaque.

Par ailleurs, en cas de fuite de données personnelles, un signalement doit être fait auprès de l'Autorité de Protection des données par le chef d'établissement endéans les 72 heures. Il est donc important de réagir rapidement.

Actions à entreprendre par le délégué référent au numérique

Prévoir des outils de détection d'incidents

Par exemple : en vous équipant d'un pare-feu et d'un bon antivirus pour aider à la détection.

S'entrainer à l'avance à reconfigurer son système en cas d'incident

La reconfiguration peut se faire à partir d'une sauvegarde, mais si celle-ci a été infectée lors d'un incident, vous devrez probablement réinstaller le système en repartant de zéro.

Déterminer (si possible) les causes de l'incident

Cela doit permettre de réparer le système, le reconfigurer, installer des patchs (correctifs) pour éviter que l'incident ne se reproduise.

Contenir l'incident

Cela peut se faire en retirant du système les appareils infectés, en limitant ou en coupant certains services à risque, en contrôlant plus attentivement les liaisons internet. Si possible, proposez un outil de remplacement aux utilisateurs concernés.

4 CHECK-LIST DES PRINCIPALES RECOMMANDATIONS À L'ÉCHELLE DE L'ÉTABLISSEMENT

Se constituer un écosystème numérique sécurisé

- ☐ Comparer les offres des fournisseurs en tenant compte des critères de sécurité
- ☐ Privilégier les outils qui limitent par défaut la récolte des données au strict nécessaire

1. Sensibiliser le personnel et les élèves[1]

- ☐ Rappeler le cadre du RGPD
- ☐ Inciter au renforcement des mots de passe
- ☐ Conscientiser aux dangers du phishing
- ☐ Rédiger une charte relative au numérique
- ☐ Conseiller des moyens de stockage sécurisés

2. Sécuriser les documents et les postes de travail

- ☐ Sécuriser les locaux sensibles
- ☐ Définir les droits d'accès, les rôles et leur obsolescence
- ☐ Réaliser les mises à jour
- ☐ Installer un antivirus et des pare-feux
- ☐ Renforcer les mots de passe
- ☐ Programmer le verrouillage automatique des sessions

3. Sécuriser le stockage des données

- ☐ Disposer de copies de sauvegardes (backups) régulièrement mises à jour
- ☐ Chiffrer les données sauvegardées
- ☐ Délocaliser le support de sauvegarde
- ☐ Utiliser des espaces de stockage en ligne sécurisés (ISO 27001)

4. Sécuriser les communications

- ☐ Distinguer usage privé/professionnel
- ☐ Ne pas partager sa boite email
- ☐ Créer un nom de domaine email professionnel pour l'équipe éducative (J.Dupont@ecole.be)
- ☐ Organiser la gestion des boites email du personnel

5. Sécuriser son réseau Wi-Fi

- ☐ Activer le chiffrement du réseau WPA2/3
- ☐ Renforcer le mot de passe Wi-Fi et le garder secret
- ☐ Dissocier les réseaux admin, enseignants, élèves…
- ☐ Éviter les réseaux Wi-Fi publics

6. Gérer les incidents

- ☐ Définir une procédure en cas d'incident et la communiquer aux membres du personnel
- ☐ Prévoir une liste de personne à contacter (ex : DPD, APD…) en cas d'incident
- ☐ Prévoir un backup (sauvegarde) exploitable et actualisé

(1) Les recommandations pourvues du symbole sont considérées comme prioritaires.

5 GLOSSAIRE

Antivirus
Logiciel qui permet de détecter les codes malveillants (virus) et de les éliminer. Par ailleurs, les logiciels antivirus fournissent une panoplie de services de sécurité complémentaires (pare-feu, chiffrement de disque dur, détection d'intrusion réseau…).

Autorité de Protection des Données
Organe de contrôle indépendant chargé de veiller au respect des principes fondamentaux de la protection des données à caractère personnel.

Backup (sauvegarde)
Copie de données (informations) que contient un terminal (ordinateur, tablette…) dans un support distinct. La sauvegarde permet de reprendre les activités de l'école normalement après avoir vécu un incident de sécurité.

CERT (La Computer Emergency Response Team)
La Computer Emergency Response Team fédérale, ou CERT.be, est le service opérationnel du Centre pour la Cybersécurité Belgique (CCB). CERT.be est chargé de détecter, d'observer et d'analyser les problèmes de sécurité en ligne ainsi que d'informer en permanence à ce sujet. Un dispositif de signalement d'incident est disponible ici :

› **cert.be/fr/signaler-un-incident**

Chiffrement
Transformation cryptographique de données, à l'aide d'un algorithme et d'un jeu de clés de chiffrement. Une fois chiffrées, les données ne sont compréhensibles qu'à la seule condition de posséder la clé de chiffrement.

Cybersécurité
Ensemble des techniques de sécurité des systèmes d'information. Il s'agit également d'un état recherché pour un système d'information lui permettant de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises (ANSSI, 2022).

Donnée à caractère personnel
Une donnée à caractère personnel est toute information se rapportant à une personne physique identifiée ou identifiable directement (exemple : nom, prénom…) ou indirectement (exemple : un identifiant sur une application, une image…).

Par exemple, une donnée à caractère personnel peut prendre les formes suivantes : les données contenues dans un Plan Individuel d'Apprentissage (PIA), les résultats des diverses évaluations externes certificatives ou non certificatives (CEB, CESS…), le données contenues dans le dossier d'un membre des personnels de l'enseignement, les profils créés sur les médias sociaux, les données traitées par des logiciels ou des applications utilisés en classe[1].

Donnée confidentielle
Une information peut être confidentielle sans nécessairement contenir une donnée à caractère personnel ou sensible au sens du RGPD.

En effet, les plans du bâtiment de l'école, les recettes et les dépenses financières de l'école, les données chiffrées relatives aux plans de pilotage sont, parmi tant d'autres, des informations auxquelles seules quelques personnes habilitées au sein d'un établissement devraient pouvoir accéder.

(1) « Guide pratique : comprendre et appliquer le RGPD en classe », disponible sur www.e-classe.be.

Donnée sensible

Donnée à caractère personnel dont le traitement est interdit, à moins d'avoir obtenu le consentement du principal intéressé et respecté les conditions prévues par le cadre du RGPD.

L'article 9 du RGPD définit les données sensibles comme suit : «…données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, …des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique… ».

Double authentification (ou identification à facteur multiple)

Méthode d'authentification qui vérifie l'identité de l'utilisateur par deux moyens différents au minimum, par opposition à la méthode traditionnelle qui n'exige qu'une seule vérification (généralement un mot de passe).

La double (ou multiple) authentification vérifie l'identité de l'utilisateur par deux des moyens suivants au minimum : ce qu'il connaît (par ex. : un mot de passe), ce qu'il possède (par ex. : son smartphone) et/ou ce qui lui est inhérent (par ex. : une donnée biométrique telle qu'une empreinte digitale).

Ainsi, il devient beaucoup plus difficile pour un pirate de se connecter au compte de sa victime, même s'il parvient à prendre connaissance de ses mots de passe.

Écosystème numérique

Ensemble intégré de services numériques accessibles à la communauté éducative d'une école. Il permet à l'utilisateur d'accéder, selon son profil et son niveau d'habilitation, à des services et à des contenus numériques.

Il offre un lieu d'échange et de collaboration entre les membres de l'équipe éducative, mais aussi avec les parents et les élèves.

Concrètement, les services offerts par les divers environnements numériques recouvrent de nombreux services utilisateurs de communication et de collaboration (courrier électronique, espaces d'échanges et de collaboration, affichage d'informations, publication web, conférence audio et vidéo), des services informationnels et documentaires (carnet d'adresses, agendas, accès aux ressources pédagogiques), des services d'accompagnement de l'élève (journal de classe, outils de suivi individuel des élèves, exercices de remédiation, affichage de l'emploi du temps), des services de production pédagogique et éducative ou encore des services utilitaires (réservation de salles et matériels, etc.).

Les écosystèmes numériques permettent également la numérisation d'un nombre croissant de procédures et d'échanges d'informations avec l'administration. (Stratégie numérique pour l'éducation, 2018)

Incident de sécurité

Événement, volontaire ou involontaire, qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien ou d'une donnée.

Exemples : incendie, panne électrique, utilisation illégale d'un mot de passe, vol d'équipements informatiques, intrusion dans un fichier ou une application, etc. (ANSSI, 2022).

ISO 27001

Norme internationale relative aux systèmes de management de la sécurité des informations. Elle a pour objet la gestion d'informations sensibles telles que les données personnelles, les données financières, les données confidentielles, etc.

Elle fait partie d'un ensemble de normes de la même famille ISO 27000 qui en compte actuellement une douzaine (comme l'ISO 27002 pour les bonnes pratiques en matière de management de la sécurité de l'information, 27701 pour la protection des données…).

Pare-feu (firewall)

Dispositif qui protège un système informatique connecté à internet des tentatives d'intrusion, notamment en cloisonnant les environnements informatiques.

Phishing (hameçonnage)

L'hameçonnage ou phishing peut être un SMS ou un mail frauduleux destiné à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance. (cybermalveillance.gouv.fr)

Rançonnement

Dans le contexte informatique, il s'agit le plus souvent d'une demande de rançon d'un pirate informatique consécutive à la subtilisation de certaines données.

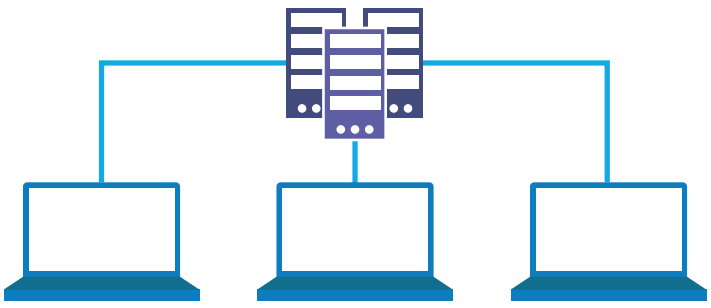
RGPD

Le règlement général sur la protection des données (RGPD) est le cadre juridique de l'Union européenne qui gouverne la collecte et le traitement des données à caractère personnel.

Serveur

Matériel informatique spécialement conçu pour fournir des informations et des logiciels à d'autres ordinateurs qui lui sont reliés via un réseau.

Il permet de mettre en relation des outils numériques (ordinateurs, imprimantes, etc.), de centraliser des données (documents, fichiers…) et des ressources (applications, imprimantes…) ainsi que de gérer les accès (authentifications, mots de passe…).



Système d'exploitation

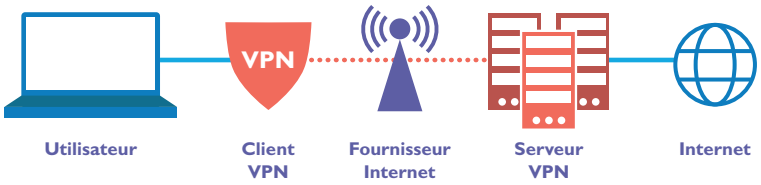
Ensemble de programmes qui assurent la gestion du fonctionnement et le contrôle d'un ordinateur. Il permet notamment d'assurer la gestion des ressources nécessaires au fonctionnement des logiciels applicatifs.

Les plus connus sont Windows (Microsoft), macOS et iOS (Apple), Android (Google), Linux (libre/open source).

VPN

« Virtual Private Network » (réseau privé virtuel en français).

Il désigne, entre autres, un tunnel virtuel sécurisé entre l'ordinateur d'un utilisateur et le serveur de son organisation.



WEP, WPA2, WPA3… (chiffrement)

Protocoles de sécurité des réseaux Wi-Fi. Il existe plusieurs protocoles dont le plus ancien qui est le WEP (Wired Equivalent Privacy), les WPA (Wi-Fi Protected Access), WPA2, WPA2 entreprise, WPA3…

Ils permettent de restreindre l'accès à un réseau Wi-Fi grâce à leur technologie de cryptage.

6 EN SAVOIR PLUS

Campagne de sensibilisation à la sécurité de l'information
Entreprise des Technologies Numériques de l'Information et de la Communication (ETNIC)
> www.youtube.com/playlist?list=PLiJ-kharAvp_NxhbPAuHNwE9ar9g4dh40

Chiffrer, garantir l'intégrité ou signer
Commission nationale de l'informatique et des libertés (CNIL)
> www.cnil.fr/fr/securite-chiffrer-garantir-lintegrite-ou-signer

Chiffrer vos documents avec Veracrypt (Tutoriel)
Commission nationale de l'informatique et des libertés (CNIL)
> www.youtube.com/watch?v=fMpzmkzAliE

Clauses contractuelles types pour le transfert de données à caractère personnel
Commission européenne
> eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CE%C2%ADLEX:32021D0914&locale=fr

Cybersécurité : Guide de gestion des incidents
Centre de Cybersécurité de Belgique (CCB)
> www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-FR.pdf

Cybersécurité : Guide pour les PME
Centre de Cybersécurité de Belgique (CCB)
> ccb.belgium.be/sites/default/files/CCB-FR%20-F.pdf
Explications plus détaillées du guide :
> cyberguide.ccb.belgium.be/fr

Guide pratique : Comprendre et appliquer le RGPD en classe
Fédération Wallonie-Bruxelles
> www.e-classe.be/resourcesingle/file/3802

jedecide.be
Autorité de Protection des Données (APD)
> www.jedecide.be

La protection des données à l'école en 7 étapes
Autorité de Protection des Données (APD)
> www.jedecide.be/sites/default/files/2018-06/La%20protection%20des%20donnees%20a%20lecole%20en%207%20etapes.pdf

Lignes directrices pour la sécurité de l'information
Autorité de Protection des Données (APD)
> www.autoriteprotectiondonnees.be/publications/lignes-directrices-pour-la-securite-de-l-information.pdf

Note relative à la sécurité des données à caractère personnel
Autorité de Protection des Données (APD)
> www.autoriteprotectiondonnees.be/publications/note-relative-a-la-securite-des-donnees-a-caractere-personnel.pdf

Rien à cacher ? Ressources pédagogiques et sources d'inspiration pour des cours sur l'importance de la protection des données
Autorité de Protection des Données (APD)
> www.jedecide.be/sites/default/files/2022-01/Rien%20%C3%A0%20cacher%20-%20importance%20de%20la%20protection%20des%20donn%C3%A9es%20-%20version%201.0_0.pdf
(consulté le 02/02/2022)

Safeonweb.be
Centre de Cybersécurité de Belgique (CCB)
> safeonweb.be

Sensibilisation au phishing (hameçonnage)
Centre de Cybersécurité de Belgique (CCB)
> www.safeonweb.be/fr/apprenez-reconnaitre-les-e-mails-frauduleux

7 RÉFÉRENCES

Agence nationale de la sécurité des systèmes d'information (2021). ***La cybersécurité pour les TPE/PME en 12 questions.***
> www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-douze-questions

Centre de cybersécurité de Belgique Cybersécurité (s. d.). ***Cybersécurité : Guide pour les PME.***
> ccb.belgium.be/sites/default/files/CCB-FR%20-F.pdf

Centre de cybersécurité de Belgique Cybersécurité (2020). ***L'ABC du CCB : la cybersécurité expliquée en 42 réponses.***
> ccb.belgium.be/sites/default/files/ABC_CCB_A5_FR.pdf

Centre de cybersécurité de Belgique Cybersécurité & Cyber security coalition Cybersécurité (2021). ***Guide de gestion des incidents.***
> www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-FR.pdf

Commission nationale de l'informatique et des libertés. ***Chiffrer, garantir l'intégrité ou signer.***
> www.cnil.fr/fr/securite-chiffrer-garantir-lintegrite-ou-signer (consulté le 31/01/2022)

Commission nationale de l'informatique et des libertés (2018). ***La sécurité des données personnelles.***
> www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

Fédération Wallonie-Bruxelles (2020). ***Guide pratique : Comprendre et appliquer le RGPD en classe.***
> www.e-classe.be/resourcesingle/file/3802

Fernandez-Toro A. (2015). ***Sécurité opérationnelle.*** **Eyrolles.**

Ghernaouti S. (2019). ***Cybersécurité : analyser les risques, mettre en œuvre les solutions*** **(6e éd.). Dunod.**

National Cyber Security Center & London Grid for Learning (2019). ***Cybersecurity : schools audit 2019.***
> www.nen.gov.uk/wp-content/uploads/2019/09/Cyber-Security-Schools-Audit-2019-NCSC-LGfL.pdf

Sophos (2021). ***The State of Ransonmware in Education 2021.***
> www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf

ANNEXES

Annexe 1 : Modèle de message d'alerte en cas d'incident

« Chers collègues, la boite à message de M… semble avoir été piratée. Il est impératif de ne pas donner suite aux emails en provenance de cette adresse email et de les supprimer. Si vous avez répondu à cet email, veuillez le signaler par téléphone dès que possible à votre chef d'établissement. »

Annexe 2 : Éléments clés d'une charte d'utilisation responsable du numérique[1]

Selon la Commission nationale de l'informatique et des libertés (CNIL - France)[2], une charte informatique devrait au moins comporter les éléments suivants :

1. Le rappel des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci.

2. Le champ d'application de la charte, qui inclut notamment :

- les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'école ;
- les moyens d'authentification utilisés par l'école ;
- les règles de sécurité auxquelles les utilisateurs doivent se conformer, ce qui doit inclure notamment de :
  - signaler à la direction toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
  - ne jamais confier son identifiant/mot de passe à un tiers ;
  - ne pas installer, copier, modifier, détruire des logiciels sur du matériel appartenant à l'école sans autorisation ;
  - verrouiller son ordinateur dès que l'on quitte son poste de travail ;
  - ne pas accéder, tenter d'accéder, ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur ;
  - respecter les procédures préalablement définies par l'école afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable de la direction et en respectant les règles de sécurité.

3. Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition comme :

- le poste de travail ;
- les équipements nomades (notamment dans le cadre du télétravail) ou partagés ;
- les espaces de stockage individuel ;
- les réseaux locaux ;
- les conditions d'utilisation des appareils personnels ;
- Internet ;
- la messagerie électronique ;
- la téléphonie.

4. Les conditions d'administration du système d'information, et l'existence, le cas échéant, de :

- systèmes automatiques de filtrage ;
- systèmes automatiques de traçabilité ;
- gestion du poste de travail.

5. Les responsabilités et sanctions encourues en cas de non-respect de la charte.

(1) Pour rédiger une politique de sécurité plus complète, se référer à la page 14 de la « note relative à la sécurité des données personnelles : la politique de sécurité » de l'APD, en suivant ce lien : www.autoriteprotectiondonnees.be/publications/note-relative-a-la-securite-des-donnees-a-caractere-personnel.pdf

(2) www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs

Fédération Wallonie-Bruxelles / Ministère
www.fw-b.be • 0800 20 000

Administration générale de l'Enseignement
Service général du Numérique éducatif
Avenue du port 16, 1080 Bruxelles
contact.sne@cfwb.be

www.enseignement.be

Rédaction : Jauad El Hasnnaoui
Graphisme : Laura Maugeri
Mai 2022

Éditrice responsable : Lise-Anne HANSE, Administratrice générale de l'Enseignement • Avenue du Port 16, 1080 Bruxelles