CONFiANCE & RESPONSABiLiTE

NUMERiQUES

Règlement Général sur la Protection des Données

ENSEIGNEMENT CATHOLIQUE
URADEL Pays de la Loire

RGPD
LES BONS REFLEXES

PLAN D'ACTION POUR LES ECOLES

INFORMATION

Etre sensibilisé à la protection des données personnelles dont j'ai la responsabilité

INVENTAIRE

Etablir la liste des données que je collecte

SECURITE

Connaître les gestes qui permettent d'assurer la sécurité des données (les miennes et celles des collègues, élèves, parents)

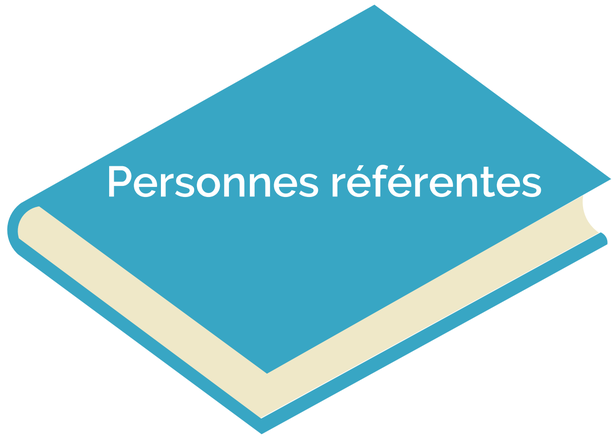
TRANSPARENCE

Bénéficier du respect de mes droits, assurer le respect des droits de mes interlocuteurs

1. INFORMATION - SENSIBILISATION

Il s'agit de présenter
le plan d'action
de l'établissement
et d'acquérir
les « bons réflexes » RGPD

- ETNA
- CANOPE
- FNOGEC/Isidoor
- CNIL



- Responsable des traitements :
  Le Chef d'Etablissement,
  en lien avec le Président OGEC
- Eventuellement : référent à la protection des données
- A la DDEC :
  Equipe cultures numériques

2. INVENTAIRE des données

1 Chacun repère les données qu'il collecte

« Ai-je créé et conservé des listes contenant des données personnelles ? »

(nom, mail, coordonnées, numéro d'identification, sexe, photo, date de naissance…)

Est-ce bien nécessaire ?

Le traitement est consigné sur un REGISTRE
(une ligne par traitement)

.

2 Chaque traitement fait l'objet d'une description

- Nature des renseignements demandés
- Auprès de qui ? (élèves, familles, personnels…) ?
- Pour quelle finalité ?
- Où sont les données ?
- Qui peut y accéder ?
- S'agit-il de données sensibles ?
- Faut-il demander un consentement ?
- Quelle durée de conservation ?

Une fiche par traitement

3. SECURITE – L'affaire de tous

« Le principal risque de sécurité identifié dans les 3 ans à venir est la cyber-criminalité liée à l'erreur humaine »

Toute fuite de données doit être journalisée en interne et déclarée à la CNIL sous 72 h

DOCUMENTS PAPIER

- Ne pas laisser traîner sur les bureaux ou dans les copieurs
- Garder sous clé

MOTS DE PASSE

- 12 caractères de 4 types différents
- Ne dit rien de vous
- Un compte = un mot de passe
- Ne pas le noter « en clair »
- Si possible double authentification
- Utiliser une phrase-clé
- Ou un gestionnaire de mdp (keepass/bitwarden)
- Ne pas enregistrer dans le navigateur
- Les changer régulièrement

EMAIL

- Ne pas envoyer de données personnelles en PJ de mail
- Utiliser un zip protégé par mdp
- Ou partager sur un drive
- Liste destinataires des mail en Cci
- Adresse mail perso distincte d'adresse mail professionnelle, éviter les redirections

ORGANISATION

Séparer les usages personnels des usages professionnels sur l'ordinateur :

création de sessions protégées par un mdp

Ne pas stocker de données sensibles sur une clé USB

Sauvegarder les données de façon sécurisée (Isidoor, NAS, disques durs externes)

PRUDENCE

Sécuriser son téléphone mobile

Se protéger des « rançongiciels »

Etre averti des techniques de phishing/hameçonnage (messages frauduleux, arnaques aux « bonnes affaires », fausses pannes d'ordinateur…)

En savoir plus : Hack-Academy

****

UN MOT DE PASSE EN BÉTON |

Un bon mot de passe doit contenir 12 caractères, d'au moins 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux. Il peut être plus court si votre compte est équipé de sécurités complémentaires !

****

IL NE DIT RIEN SUR VOUS |

Personne ne doit deviner votre mot de passe à partir du nom de votre chien ou de votre film préféré. Idem pour le code de votre smartphone : préférez un nombre aléatoire à une année.

****

UN COMPTE, UN MOT DE PASSE |

Pour éviter les piratages en cascade, chacun de vos comptes en ligne qui présente un caractère sensible (banque, messagerie, réseau social, etc.) doit être verrouillé avec un mot de passe propre et unique.

****

NE JAMAIS L'ABANDONNER EN PLEINE NATURE |

Les post-it, les fichiers texte, votre smartphone ou votre boite de messagerie ne sont pas conçus pour sécuriser le stockage de vos mots de passe. Pensez aussi à ne jamais les enregistrer dans le navigateur d'un ordinateur partagé.

****

DEUX CADENAS VALENT MIEUX QU'UN |

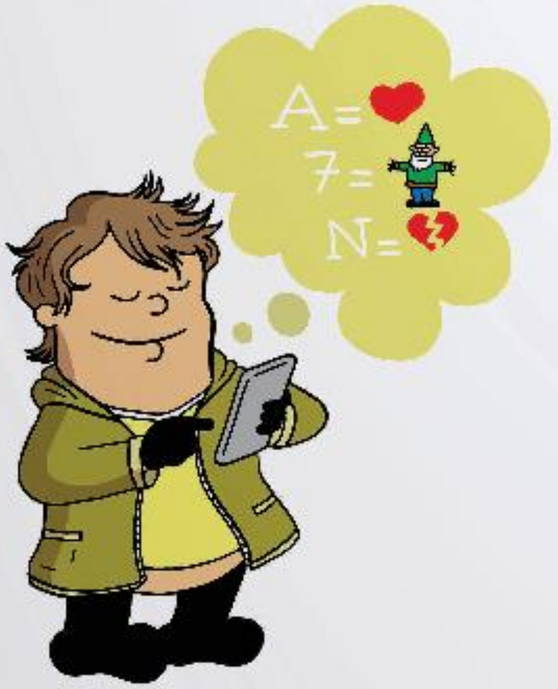
Quand le service vous le propose, activez la double authentification. Si quelqu'un se connecte à votre compte depuis un terminal inconnu, le site vous prévient par SMS/e-mail. Libre à vous d'autoriser ou de refuser l'accès !

****

LES RETENIR SANS LES ÉCRIRE

… EN TRAVAILLANT VOS NEURONES |

Mémorisez une phrase puis utilisez la première lettre de chaque mot pour créer votre mot de passe. La phrase doit contenir des chiffres et des caractères spéciaux !



****

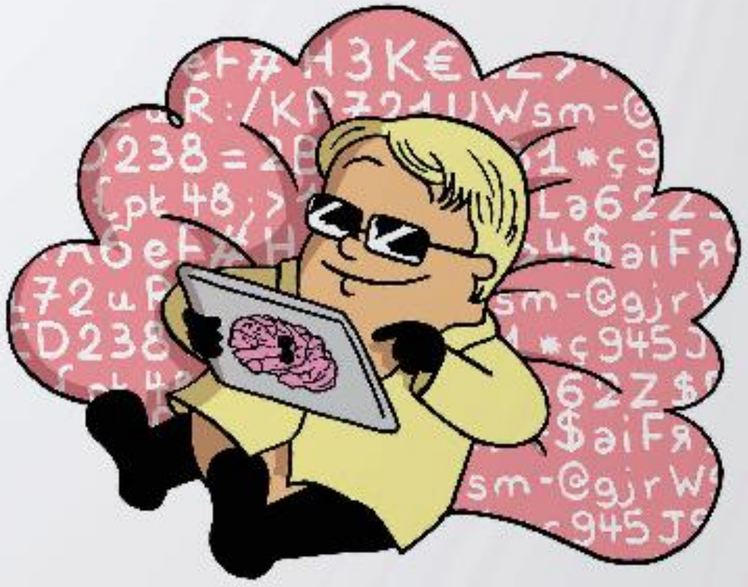
PLUS DE CONSEILS SUR WWW.CNIL.FR

CNIL.

COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

… EN REPOSANT VOS MÉNINGES |

Utilisez un gestionnaire de mots de passe ou un trousseau d'accès chiffré pour stocker vos mots de passe en toute sécurité. Vous n'aurez à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes !



Illustrations : Martin Vidberg

4. TRANSPARENCE

Respecter les droits des personnes et leur accès aux données qui leur appartiennent

01 **Charte d'utilisation du numérique**
Pour les personnels
Pour les élèves

02 **Mentions légales sur les formulaires**
Cf modèles communiqués sur le site « Guide RGPD 1D »
Mention de conformité, case à cocher pour le consentement
Personne à contacter pour exercer le droit d'accès aux données

03 **Déclaration de protection de la vie privée**
Cf modèle communiqué sur le site « Guide RGPD 1D »

04 **Mise à jour du contrat de scolarisation**
Isidoor – clauses à vérifier

05 **Mise à jour des contrats de travail**
Clause de confidentialité…
Cf Isidoor application Social

06 **Prévoir les modalités d'exercice des droits des personnes**
concernées par les traitements identifiés
(droit d'accès, de rectification, retrait du consentement…)

SYNTHESE DU PLAN D'ACTION

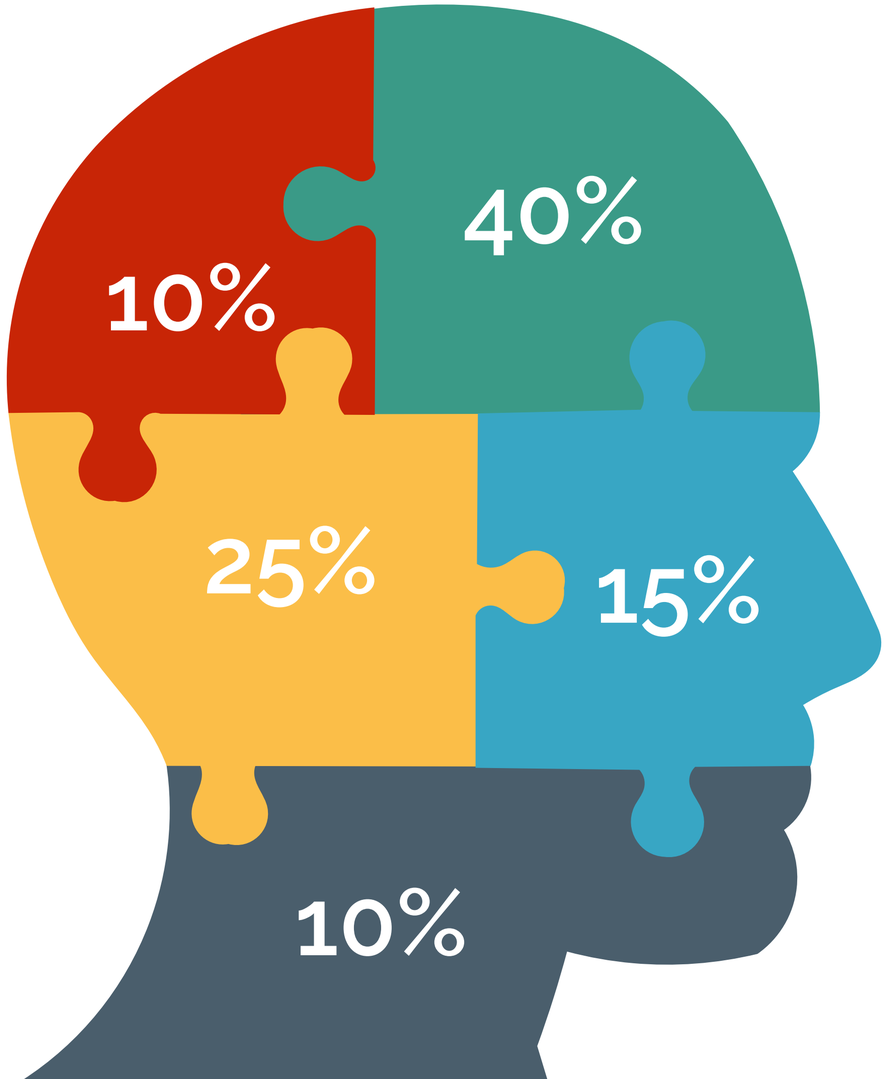
01
INFORMATION

02
INVENTAIRE

03
SECURITE

04
TRANSPARENCE

05
BONS REFLEXES



Questions ?