Règlement Général sur la Protection des Données
Guide des bonnes pratiques pour le personnel enseignant, éducatif et administratif des établissements

Pour le personnel enseignant, éducatif et administratif de l'établissement	
Activités	**Bonnes pratiques**
Communication professionnelle par messagerie électronique entre les services administratifs, vie scolaire et les enseignants.	- La communication par messagerie électronique doit se faire exclusivement par le biais de la messagerie académique. - Aucune copie ni redirection automatique d'une boîte de messagerie professionnelle vers une boîte de messagerie privée ne DOIT être autorisée. Vous engagez votre responsabilité lorsque vous mettez en place ce type de pratique. - Configurer un logiciel de messagerie vous permet d'utiliser (consulter et écrire) votre messagerie professionnelle en toute sécurité sans risque de détournement de données personnelles pour lequel notre responsabilité individuelle est engagée. - Dans la messagerie professionnelle, les messages privés DOIVENT être identifiés comme tel sur la messagerie professionnelle, par exemple en mettant « [PRIVÉ] » ou « [PERSONNEL] » en tête du sujet, voire « [MESSAGE PRIVÉ] - Les éventuelles adresses privées des agents ne DEVRAIENT pas être utilisées pour les activités pédagogiques ou administratives. - L'expéditeur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages. **Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés** afin d'éviter les diffusions de messages en masse. - ***Le champ [Cci…]*** *: (copie cachée à)* *Si vous voulez envoyer un message à des destinataires de manière à ce que la confidentialité des adresses de messagerie de chacun soit respectée, utilisez uniquement le champ [Cci…].* *Comme la plupart des messageries exigent qu'il y ait au moins une adresse dans le champ [À…], entrez votre propre adresse pour éviter que vos destinataires s'interrogent sur l'émetteur du message. Cette utilisation permet en outre d'éviter la propagation des messages pourriels (SPAM).* *Exemple : un message adressé à l'ensemble des parents d'une même classe.*

Document élaboré avec la collaboration du groupe de travail du sud et finalisé avec l'équipe RGPD du Collège Terre Sainte.

Activités	Bonnes pratiques
Communication avec les élèves dans le cadre des activités pédagogiques et de leur organisation. Communication avec les parents ou responsables légaux dans le cadre professionnel	- Utiliser la messagerie pédagogique (interne à l'ENT) - Les éventuelles adresses privées des élèves ne DEVRAIENT pas être utilisées pour les activités pédagogiques ou administratives.
Échange de documents entre les membres de la communauté éducative	- Privilégier les outils académiques (Owncloud, FileZ(avec code accès), FileSender) - Pronote (éditeur privé, autorisé par le responsable de traitement)
Échange de documents et communication avec les élèves	- Privilégier les outils de l'ENT (Pydio, Owncloud, messagerie pédagogique, cours en ligne), Pronote (autorisé par le responsable de traitement)
Utilisation des postes de travail de l'établissement	- **Ne jamais utiliser un poste de travail sans s'être authentifié avec SON identifiant et mot de passe.** - S'obliger à changer régulièrement son mot de passe d'accès au réseau pédagogique. - Ne jamais confier son identifiant/mot de passe à un tiers - Verrouiller son ordinateur dès que l'on quitte son poste de travail - **Fermer sa session en quittant son poste de travail** - Sauvegarder ses données personnelles sur le serveur sécurisé dans le dossier « privé » - Un poste de travail peut contenir des données personnelles, voire privées, d'un utilisateur. L'utilisateur DOIT identifier ses données en les marquants par les mots "PERSONNEL" ou "PRIVÉ". - Les clés USB peuvent être des vecteurs d'infections du réseau, les enseignants doivent s'assurer que leur clé USB n'est pas infectée avant de la connecter au réseau du collège.
Connexion de son ordinateur personnel (BYOD) au réseau de l'établissement	- **Demander l'aval de l'équipe informatique de l'établissement avant de connecter son ordinateur personnel sur le réseau.** - S'assurer de disposer d'un antivirus à jour avant de le connecter - Désactiver les services de synchronisation des clouds privés - Verrouiller son ordinateur dès que l'on quitte son poste de travail
Traitement des données personnelles sur son équipement informatique personnel ou BYOD (Portable, Poste fixe,	- Prévoir une sauvegarde des données, en dehors des clouds privés. - Prévoir des moyens de chiffrement des postes nomades et supports de stockage amovibles

Smartphone ou tablette) et sur les périphériques de stockage (clé USB, disque dur)	- Prévoir une sauvegarde des données, en dehors des clouds privés. - Prévoir des moyens de chiffrement des postes nomades et supports de stockage amovibles
Visualisation des vidéos issues des sites de streaming (youtube, dailymotion , vimeo , ..)	- **Vérifier la licence d'utilisation** - Cas particulier de YouTube : en cas de streaming **autorisé**, privilégier l'intégration de la vidéo en activant le mode de confidentialité avancé (pas d'utilisation de cookies pour suivre les pages vues par les utilisateurs) - Si difficulté de streaming, téléchargement au préalable des vidéos **autorisées**
Capture de photo, vidéo et audio des élèves	- Faire remplir les autorisations de diffusion (droit à l'image – Internet responsable) - Consigner et archiver les autorisations - les photos des élèves ne doivent pas être conservées au-delà de la période fixée par la demande d'autorisation signée par les représentants légaux (généralement 1 an). Passé ce délai, les photos doivent être supprimées des ordinateurs, tablettes ou sites Internet.
Utilisation d'une application ou d'un service en ligne qui ne se trouve pas dans l'ENT et/ou Le GAR	- **Suivre le process de versement au registre de l'EPLE pour savoir si l'usage de l'application est/sera autorisé par le responsable de traitement.** - Lire les Conditions Générales d'Utilisation et/ou la politique de confidentialité de l'application pour vérifier que cela ne nécessite pas l'externalisation des données personnelles des élèves - Privilégier en premier lieu la création de comptes anonymes pour un usage de l'application SANS donnée à caractère personnel ou des comptes avec pseudonymes.
Responsabilisation des élèves dans l'exercice (futur) de leur majorité numérique	- Formation des élèves par le biais d'activités issues d'une progression allant **du cycle 3 au cycle terminal** - **Se reporter au référentiel de la CNIL** https://eduscol.education.fr/cid129745/le-referentiel-cnil-de-formation-des-eleves-a-la-protection-des-donnees-personnelles.html