ACADÉMIE
DE TOULOUSE

Liberté
Égalité
Fraternité

PRESENTATION NOUVEAUX ARRIVANTS

Personnels enseignants

Gilles Garrouty– Directeur régional adjoint et responsable de la sécurité des systèmes d'information adjoint

ACADÉMIE
DE TOULOUSE
Liberté
Égalité
Fraternité

Sommaire

1. L’identité numérique

Identité Numérique professionnelle des agents

À son arrivée, l'académie de Toulouse met à votre disposition une identité numérique professionnelle et une boîte aux lettres électronique institutionnelle individuelle.

- Les courriers électroniques de la communauté administrative et éducative, académique et nationale seront transmis à cette adresse. La nature sensible des informations reçues à cette adresse impose une vigilance quant à l'usage de cette boîte aux lettres numérique.
- Un service de messagerie, avec un annuaire académique , est également mis à disposition, ces services sont synchronisables sur vos équipements personnels pour éviter le transfert sur des boites externes.
- L'identité numérique professionnelle est associée à un couple identifiant et mot de passe appelé compte d'identification personnel ; Ce compte est unique et vous permet d'accéder à tout votre environnement numérique
- Le personnel se connecte sur https://mamamia.ac-toulouse.fr/ et génère **son propre mot de passe**

Gestion de mon compte académique

Un espace dédié à l'identité numérique existe Module d'Aide à la Maintenance Individuelle Automatique

MaMamia est une application académique reliée à l'identification des personnels de l'académie de Toulouse: https://mamamia.ac-toulouse.fr

- De connaître ou de retrouver l'identifiant et l'adresse email principale de son compte académique
- De définir son premier mot de passe lors de son arrivée dans l'académie
- De redéfinir son mot de passe si on l'a perdu
- De modifier son mot de passe lorsqu'on souhaite le renouveler

Compte de messagerie

L'académie de Toulouse met à disposition de tous les personnels une boîte aux lettres électronique

Adresse de messagerie :

prenom.nom@ac-toulouse.fr

éventuellement suivi d'un chiffre en cas d'homonyme

Ce compte de messagerie correspond à **votre identifiant numérique académique. Il vous permettra également d'accéder à toutes les applications nationales et académiques accessibles depuis le portail métiers Arena.**

Il vous sera demandé de renseigner :

- votre **identifiant** : **pnom** (1ère lettre du prénom suivi de votre nom, et éventuellement d'un chiffre)
- votre **mot de passe** : **XXXXX**, personnel et à usage unique.

Compte de messagerie

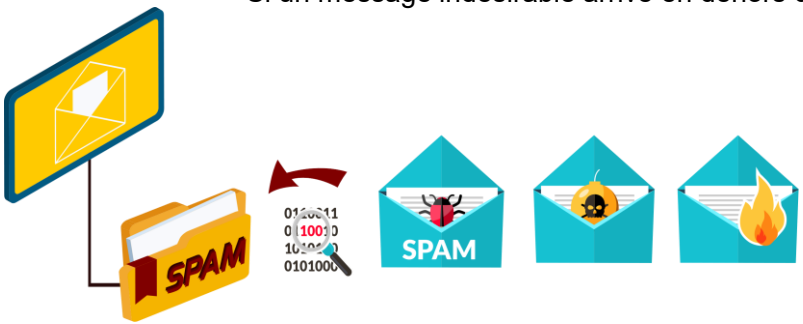
Vous **NE DEVEZ PAS** transmettre vos identifiants et mots de passe à une tierce personne

L'adresse mail que l'académie fournie est **professionnelle**.

→ La **nature sensible des informations** reçues à cette adresse impose une vigilance quand à l'usage de cette boîte aux lettres numérique.

Gestion des SPAM

Si un message indésirable arrive en dehors du dossier prévu → **spam@ac-toulouse.fr**



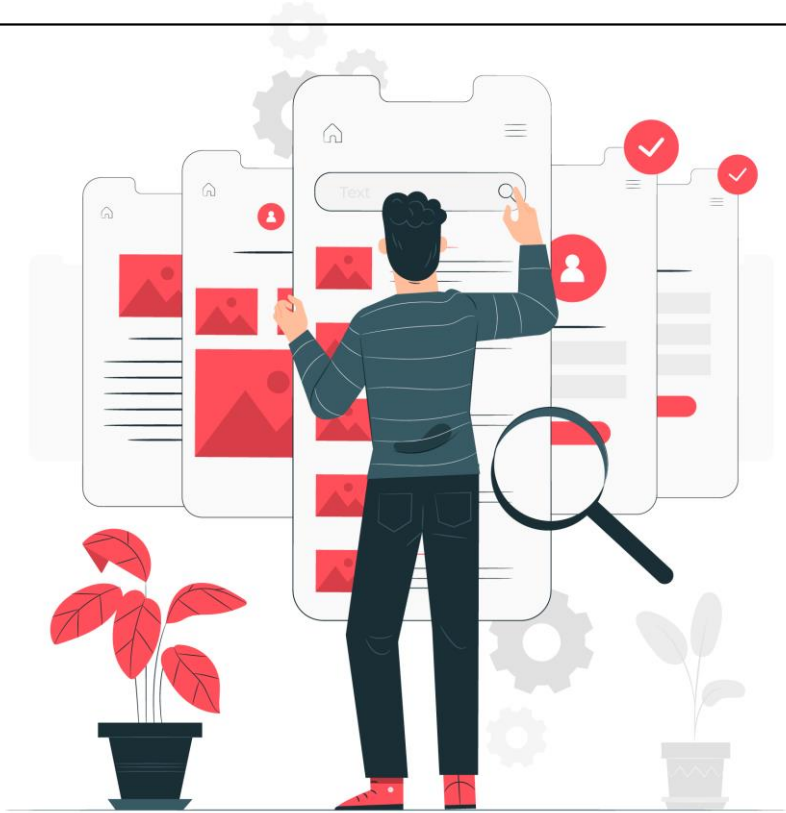
EduConnect

EduConnect est un service d'authentification créé pour simplifier les démarches des usagers de l'éducation nationale et l'accès aux services numériques de l'école au lycée. Il **simplifie pour les parents l'accès au suivi et à l'accompagnement de la scolarité des enfants et donne accès pour les élèves à l'ensemble des services numériques de l'école au lycée.**

Tout **élève** ou **représentant légal** dispose d'un compte **EduConnect** dès l'inscription dans un établissement scolaire public

Pour utiliser le compte, il suffit de se connecter à l'adresse https://educonnect.education.gouv.fr/ avec ses identifiants EduConnect (générés par la plateforme pour le représentant légal et communiqués par l'établissement pour l'élève) ou d'utiliser ses identifiants FranceConnect.

2. Les outils numériques



Portail Métier

Le portail Arena (depuis l'extérieur) vous donne accès aux applications professionnelles, en fonction de votre profil (enseignant, professeur principal …) ou de vos droits délégués.

Par exemple : les applications de formation comme M@gistère, l'accès au PAF, les applications RH, comme I-prof, e-colibris, le portail des démarches RH Colibris, la gestion de la scolarité ou des crédits du pass culture.

L'accès à l'ENT à venir ou l'accès aux communs numériques Apps

Un bouquet de services
I-Prof
pour les enseignants

Colibris

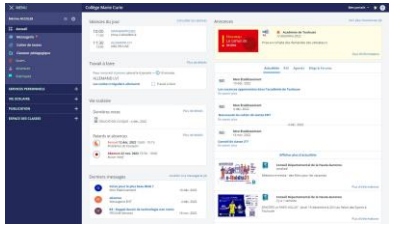
pass Culture

m@gistère

Portail ENT

L'espace numérique de travail (ENT) des établissements pour la scolarité: communication; services pédagogiques (cahier de textes; classeur pédagogique; travail en ligne); services de vie scolaire (absences; bulletins).

Disponible pour tous les établissements du 2nd degré à partir d'une des deux plateformes réalisées par le même éditeur et à ce jour pour 36% des écoles pour le 1er degré



ENT école

mon ent occitanie

collège 31 HAUTE-GARONNE

Portail Scolarité Services

Il comprend l'ensemble des démarches en ligne pour les élèves et les représentant légaux, et permet:

- de faciliter et centraliser les démarches administratives ponctuelles liées à la scolarité des enfants (exemple : inscription au collège et au lycée, demande de bourses, demande d'orientation, affectation après la 3e, paiement des factures…) ;

- de permettre un suivi de la scolarité grâce au service de consultation du livret scolaire ou d'autres services qui peuvent être choisis par les établissements (consultation du cahier de texte, de l'emploi du temps…).

Communs Numériques

Une nouvelle plateforme, Apps, vous propose l'accès à des services numériques partagés à l'échelle nationale :

Nuage est une plateforme d'hébergement et de partage de fichiers et d'édition collaborative dans le cloud.
Une capacité de 100Go par utilisateur.
L'installation de l'application en local permet la synchronisation particulièrement intéressante en mode déconnecté
Répond également à des besoins de partages entre quelques utilisateurs internes ou externes

Tchap : Messagerie instantanée interministérielle sécurisée
Application conçue en France, cryptée et que l'on peut installer sur ses appareils mobiles (tablettes, téléphones) ou fixes.

Evento permet de planifier des événement à plusieurs.

Tribu est une plateforme gérant des espaces de travail collaboratif
Tribu permet à un groupe d'utilisateurs de la communauté de partager des documents, des agendas, des taches, des forums de discussion.
Il offre la possibilité d'être libre de son organisation et permet de travailler en ligne.

Communs Numériques

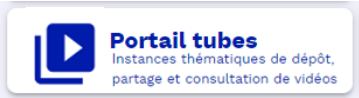
Visio-Agents
Service de visioconférence

Visio-agents est un service de visioconférence pour des réunions entre agents
La présentation dans Eduscol

Classe virtuelle d'Occitanie
Service de classe virtuelle pour la continuité pédagogique

Classe virtuelle d'Occitanie est un service pour organiser des classes virtuelles avec ses élèves dans le cadre la continuité pédagogique.

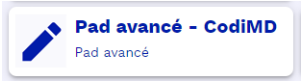
Communs Numériques



PeerTube permet de déposer, d'héberger et de consulter des média audios et vidéos.
Il vous permet de les référencer efficacement par la création de 'chaînes' à partager à vos élèves.
Basée sur le logiciel libre PeerTube.

Pod Educ est une plateforme de dépôt, d'enrichissement et de consultation de vidéos à destination de tous les agents.
Similaire à Portail tubes, avec ceci en plus qu'elle autorise la création de versions enrichies de ces vidéos en ajoutant des sous-titres, en associant des documents ou en proposant des chapitres.
On peut également intégrer du texte, des images, apporter des annotations timecodées aux vidéos. Cela lui confère un usage plutôt orienté "mooc".
La création directe de capsules vidéos est possible, en enregistrant son écran et son micro.

Communs Numériques



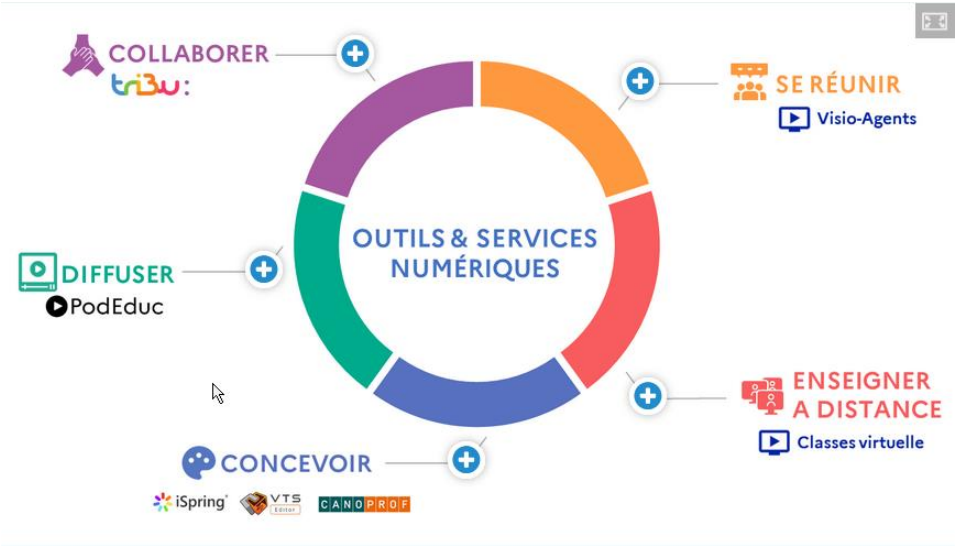
CodiMD est un éditeur de texte en MarkDown
Cet éditeur permet de créer des documents directement en ligne, en mode collaboratif. Il permet une mise en forme basique (gras, souligné, etc.), en gérant des documents qui utilisent la syntaxe MarkDown, ce qui permet l'édition de code informatique par exemple.
Il supporte également le copier-coller depuis des documents bureautiques ou des pages web.

Filesender permet l'échange de fichiers volumineux
Le transfert est possible jusqu'à 100 Go via une interface web.
Une invitation mail ou un lien URL vous permet de les rendre disponibles au téléchargement pour n'importe quel utilisateur de la communauté éducation-Recherche ou toute personne extérieure.
Afin d'apporter une sécurité optimale à vos fichiers sensibles, vous avez la possibilité de les chiffrer lors du dépôt via un mot de passe, généré automatiquement ou personnalisé.

FranceTransfert permet l'échange de fichiers volumineux
France transfert est un service créé par l'Etat pour aider ses usagers à envoyer ou recevoir des agents de l'Etat des fichiers et dossiers volumineux qui ne peuvent pas transiter par les messageries électroniques.
Comme FileSender, France transfert permet d'envoyer des fichiers volumineux non sensibles de manière sécurisée

Communs Numériques

Services numériques pour l'agent



Un nouveau parcours d'accompagnement à l'usage de services numériques : "Services numériques pour l'agent" proposé par le pôle FOAD : cliquez ici

Ce parcours comporte aujourd'hui 6 modules présentant Tribu, Visio-agents, Classe virtuelle, PodEduc, des outils de conception et le portail Apps. Il a vocation à être étoffé et mis à jour de façon continue.

Portail pédagogique

Le portail pédagogique de l'académie de Toulouse est un espace de mutualisation des pratiques pédagogiques innovantes, répondant aux nouveaux enjeux de l'École en faveur de la réussite des élèves.

Il se compose d'un ensemble de sites disciplinaires alimentés par les contributions de divers acteurs de terrain, et donne accès à de nombreuses ressources pédagogiques et didactiques pour l'école, le collège et le lycée, visant notamment à accompagner les pratiques transversales.

https://disciplines.ac-toulouse.fr

2. Sécurité

Qu'est-ce que la SSI ?

SSI : Sécurité du Système d'Information

- Pas de SSI → Pas de SI

PSSI : Politique de Sécurité du Système d'Information

- Indispensable: impact sur l'image, le service, juridique, organisationnel
  Objectif : réduire les risques et limiter les impacts
- Elle définit les éléments stratégiques et les règles de sécurité organisationnelles et techniques qui ont pour objectifs le maintien de **l'intégrité, la disponibilité et la confidentialité de l'information**.
- Elle impose la mise en œuvre de
  - dispositifs et procédures techniques : pare-feu, techniques de chiffrement, antivirus etc...
  - la sensibilisation et l'information des utilisateurs au travers de chartes, de guide de bonnes pratiques, de rencontres

Qu'est-ce que la SSI ?

Preuve

Toute évolution/modification de la donnée doit être tracée pour permettre «l'auditabilité».

Le cadre réglementaire de la SSI est soumis à de nombreux textes de toute nature.
•La jurisprudence y est très présente.
•Il est en perpétuelle évolution.

- Loi Godfrain - 1988 Fraude informatique
- Le code de l'éducation juin 2000
- Loi d'Orientation et de programmation de sécurité Intérieure (LOPSI) 2002
- 2004 circulaire Darcos protection des mineurs
- Loi pour la confiance dans l'économie numérique (LCEN) 2004
- Loi pour la lutte contre le terrorisme 2006
- Loi téléchargement (Hadopi) 2009
- Loi d'Orientation, de programmation et de performance de sécurité Intérieure (LOPPSI 2) 2011
- Loi sur le secret des correspondances 2011
- Politique de sécurité des systèmes d'information de l'État 2014
- Règlement 2016/679 (RGPD) 2018

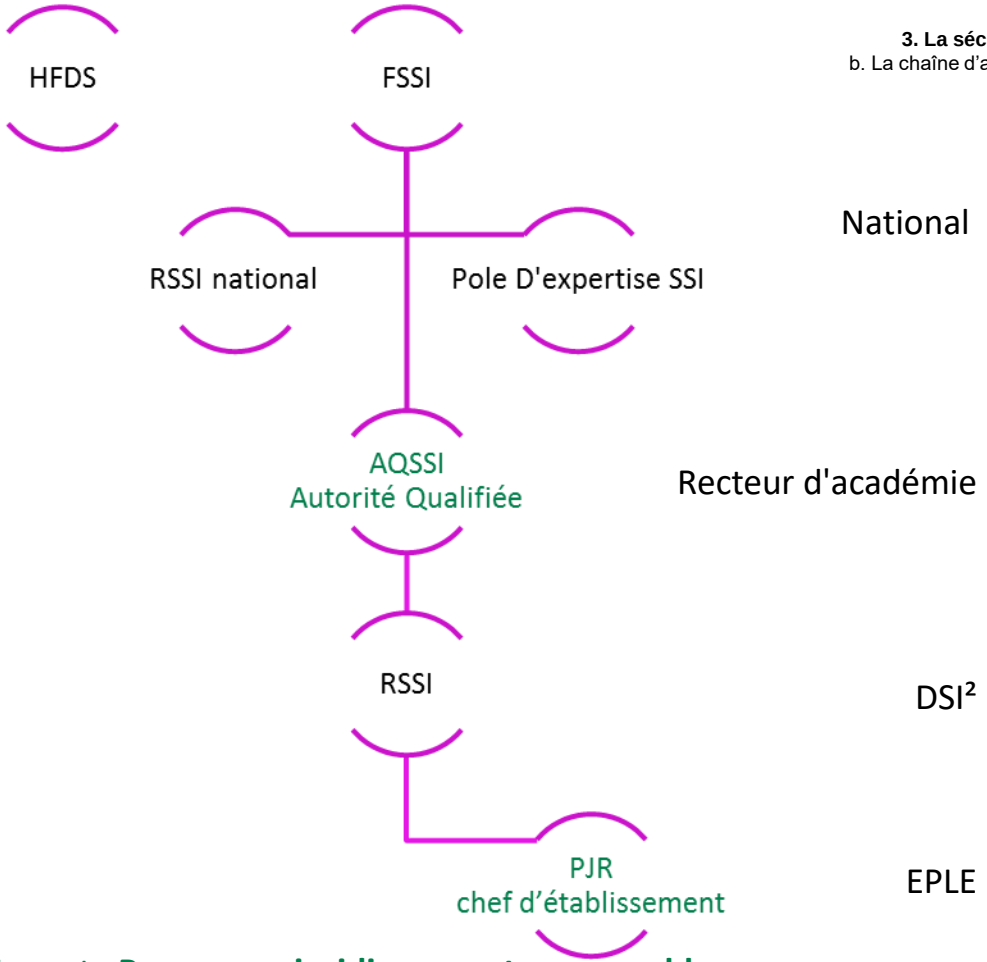
La chaîne d'alerte

Une chaîne d'alerte a été définie permettant d'engager les mesures adaptées dans les meilleurs délais et d'assurer la circulation de l'information utile afin de maintenir un niveau de protection optimal.

Dans l'académie, elle peut être saisie sur le centre de services

Domaine de service	Groupe de famille	Famille de service	Service	Sous catégorie de service
Réseaux, infrastructure et sécurité	Sécurité	Incident	Alerte de sécurité	Alerte de sécurité
Réseaux, infrastructure et sécurité	Sécurité	Conseil - Expertise	Alerte de sécurité	Alerte de sécurité
Réseaux, infrastructure et sécurité	Sécurité	Aide usages - Données	Alerte de sécurité	Alerte de sécurité

ou en écrivant à **rssi@ac-toulouse.fr**



En vert : **Personnes juridiquement responsables**

La chaîne d'alerte

A quel moment alerter ? Si un incident de sécurité est détecté :

Un incident de sécurité est un événement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien.
Exemples : utilisation illégale d'un mot de passe, vol d'équipements informatiques, intrusion dans un fichier ou une application, etc. (source : ANSSI)

- Usurpation de ressources
- Saturation ou perturbation du système informatique ou du réseau
- Intrusion
- Divulgation de données sensibles
- Non respect des recommandations et règles de sécurité
- Vol ou perte d'un équipement informatique
- Téléchargements illégaux

L'information des autorités hiérarchiques et du RSSI est **obligatoire** lorsque l'incident peut mettre en cause l'entité dans son fonctionnement, sa sécurité, sa discipline interne, son image. Elle est **impérative** si l'incident est susceptible d'implications juridiques.

Circulaire ministérielle N 2004 035

Mettre en place des contrôles :

- a priori des informations consultées, en interdisant l'accès à un ensemble de sites reconnus comme inappropriés
- à posteriori, par examen de la liste des sites consultés

Informer et sensibiliser les élèves et les personnels à l'usage d'Internet.

Établir une charte d'utilisation de l'Internet et l'annexer au règlement intérieur.

Les chartes en établissement

Charte EPLE : cf. exemple de charte
https://eduscol.education.fr/chrgt/S2i2e-charte.pdf

- **Comment élaborer la charte**
Instances participatives de l'établissement : conseil d'administration, conseil pédagogique, commission permanente, conseil de la vie lycéenne, réunion des délégués des élèves dans les collèges.

-> valider en conseil d'administration et adosser au règlement intérieur

- **Constitution** de la **charte**
  - pourquoi une charte
  - description des services en ligne offerts par l'établissement et de leurs modalités d'accès et d'utilisation
  - modalités selon lesquelles les droits et obligations des usagers trouvent à s'appliquer lors de l'usage des TIC
- **Diffusion** de la **charte**
  - équipe pédagogique et élèves
  - et la faire **signer**
- Prévoir des sanctions dans le règlement intérieur
- Penser à la réviser régulièrement : les usages et la règlementation évoluent.

Charte académique

Vigilance en établissement

Directeur de publication

- Droit à l'oubli (2004) : à l'origine la loi informatique et liberté (art 6) protège les données d'une personne
- Conservation des données : doit être pour une durée qui ne dépasse pas ce pour quoi elles ont été collectées
- Copyright, contrefaçon
- Mention légales

Autre rôle du chef d'établissement

- Information et formation des enseignants, apprendre aux élèves les opportunités, savoir protéger leur image, leur vie privée.
- Familles : Sujet doit être abordé avec eux. Les parents sont pénalement responsables jusqu'à la majorité de leur enfant. Il est nécessaire de former les parents.
- Responsable de Traitements (RGPD)

3. RGPD

Le Règlement Général pour la Protection des Données

DPD M. Roussel Bruno Roussel

- Pour les établissements : M. Roussel est déclaré auprès de la CNIL comme DPD de l'établissement

RSSI : Responsable de la Sécurité du Système d'Information

- RSSI de la région académique Occitanie : Nicolas Barachet
- RSSI adjoints : Hervé Mirabail, Gilles Garrouty, Cédric Deville

La sécurité informatique est l'affaire de tous.
La sécurité doit être abordée d'une manière globale.
La sécurité est un processus continu
Les mesures de sécurité doivent répondre aux besoins de sécurité exprimés au regard des risques.

Contexte

Le règlement général sur la protection des données (RGPD) crée un cadre de confiance et renforce les droits des usagers quant à l'utilisation de leurs données à caractère personnel.

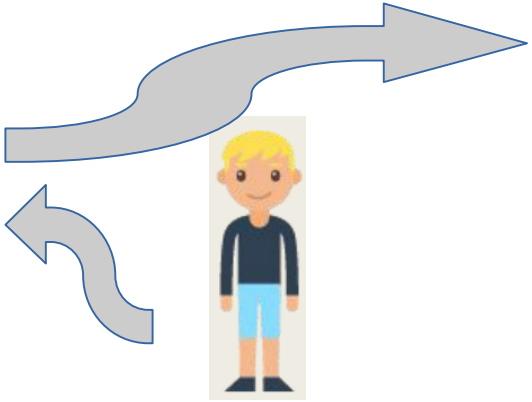
Dans le domaine de l'éducation il ne s'agit pas de se priver des innovations technologiques si elles apportent une réelle plus-value pédagogique mais il convient de ne pas transiger sur les principes éthiques.

Dans chaque académie un délégué à la protection des données (DPD) veille au respect du cadre légal concernant la protection des données.

Les acteurs

L'enseignant

Se questionne lorsqu'il choisit un nouvel outil et applique la **démarche ci-après**.

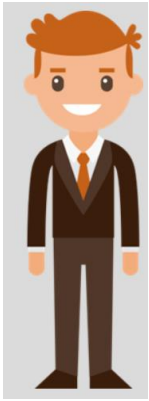


Les élèves

Au sens du RGPD, l'élève est la **personne concernée**.
On se doit de **protéger ses données personnelles**.

Le(a) chef(fe) d'établissement

C'est le **responsable de des traitements de données à caractère personnel** dans son établissement.
Son rôle:
• **Garantit la conformité** au RGPD
• **Tient des registres** (traitement et violations)



Le DPD

-**Sensibilise**, informe, conseille les chefs d'établissement
-**Veille au respect** de la mise en œuvre du **RGPD**
-**Traite les incidents** et les réclamations des usagers
-**Coopère** avec la **CNIL**

10 principes clés

1- Bien choisir ses outils

Privilégier l'usage de logiciels libres, des outils développés ou encadrés par le ministère (ENT, GAR...)

Utiliser de préférence des logiciels ou applications hébergés dans l'Union européenne

Informer le chef d'établissement ou le directeur d'école de l'utilisation en classe d'une ressource collectant des données personnelles afin de compléter le registre des traitements

Lire attentivement les informations disponibles sur les sites pour savoir si des données personnelles sont collectées, à quelles fins, et être vigilant à ce qu'aucune réutilisation commerciale ne soit envisagée

Vérifier que les parents et les élèves sont informés du traitement de leurs données personnelles et de la possibilité d'exercer leurs droits (d'accès, de rectification, etc.)

10 Principes Clés

2 - Protéger les données des élèves dans toute activité pédagogique

Limiter toute collecte de données personnelles aux informations indispensables au bon déroulement de l'activité puis veiller à ce qu'elles soient supprimées ou archivées selon la réglementation (au-delà de la durée nécessaire à l'activité)

Respecter le droit à l'image des élèves et les droits d'auteur

Sensibiliser les élèves aux enjeux de la protection des données personnelles

Créer des pseudos lors des activités pédagogiques en ligne si l'utilisation de l'identité de l'élève n'est pas nécessaire

S'assurer de la sécurité des données collectées notamment grâce à des mots de passe et à un antivirus

Où s'informer ?

Pour prendre conseil auprès d'un délégué académique à la protection des données : https://education.gouv.fr/RGPD

RESSOURCES :

Site du ministère de l'Éducation nationale
Site educscol

Infographie : les 10 principes clés

Le guide de survie de l'enseignant

Un guide et des activités pour les élèves, mais pas seulement…

Un parcours M@gistère pour découvrir le RGPD

4. Bonnes pratiques

Bonnes pratiques

La sauvegarde :

- Sécuriser ses données en cas d'incident
- Utiliser les partages réseaux
- NE PAS UTILISER les sauvegardes dans le cloud (Dropbox, iCloud, Google Drive, …):
  - risques pour la confidentialité des données,
  - risques juridiques liés à l'incertitude sur la localisation des données,
  - risques liés à l'irréversibilité des contrats.

-> Nuage : Solution souveraine de stockage en ligne et de synchronisation de fichiers (100 Go)
L'édition en ligne est possible grâce aux outils open Source intégrés, ce qui permet de collaborer avec ses élèves et d'envisager des usages pédagogiques sans utiliser les plateformes non RGPD.

LES MOTS DE PASSE

Votre mot de passe doit être différent pour chaque service, suffisamment long et complexe, et impossible à deviner. Ne le communiquez jamais à un tiers. Pour votre messagerie, il doit être particulièrement robuste.

LA SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

Protégez l'accès à vos comptes, vérifiez vos paramètres de confidentialité et maîtrisez vos publications. Faites attention à qui vous parlez. Vérifiez régulièrement les connexions à votre compte.

LA SÉCURITÉ DES APPAREILS MOBILES

Mettez en place les codes d'accès. Appliquez les mises à jour de sécurité et faites des sauvegardes, évitez les réseaux Wi-Fi publics ou inconnus. Ne laissez pas votre appareil sans surveillance.

LES SAUVEGARDES

Pour éviter de perdre vos données, effectuez des sauvegardes régulières. Identifiez les appareils et supports qui contiennent des données et déterminez lesquelles doivent être sauvegardées. Choisissez une solution adaptée à vos besoins. Protégez et testez vos sauvegardes.

LES MISES À JOUR

Mettez à jour sans tarder l'ensemble de vos appareils et logiciels. Téléchargez les mises à jour uniquement depuis les sites officiels et activez l'option de téléchargement et d'installation automatique des mises à jour.

LES USAGES PRO-PERSO

Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez. Ne mélangez pas votre messagerie professionnelle et personnelle et n'utilisez pas de service de stockage en ligne personnel à des fins professionnelles.

COMPRENDRE LES RISQUES ET RÉAGIR

L'HAMEÇONNAGE

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

BUT
Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE
Leurre envoyé *via* un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

LES RANÇONGICIELS

EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

BUT
Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE
Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

ESCROQUERIE FINANCIÈRE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

BUT
Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants

TECHNIQUE
Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.).

COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels

- Ne répondez pas
- Conservez toutes les preuves
- Redémarrez votre appareil
- Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur
- Désinstallez tout nouveau programme suspect
- Faites une analyse antivirus
- Changez tous vos mots de passe
- Faites opposition auprès de votre banque si vous avez payé
- Déposez plainte

5. Accompagnement

Accompagnement

- **Espace DSI**

Sécurité des systèmes d'information (SSI)
lien : https://dsi.ac-toulouse.fr/la-dsi/securite-des-systemes-dinformation-ssi

Cyber sécurité
lien : https://dsi.ac-toulouse.fr/quest-ce-que-la-cybersecurite

- **Centre de services**

Mon Univers de SErvices

Portail web Arena
Onglet "***Support et Assistance***" puis "***Assistance académique***"

Site de la DSI -> https://dsi.ac-toulouse.fr

Actualité concernant la DSI
Les informations pratiques
Les bonnes pratiques
Les liens vers les outils : environnent de travail, applications métiers, téléphonie

Edulab

La direction de région académique du numérique pour l'éducation de la région académique Occitanie est présente sur l'ensemble de l'académie de Toulouse dans des « EduLAB », des lieux de co-formation animés par un « référent EduLAB ». Il s'agit d'un enseignant du second degré possédant une expertise du numérique au service des apprentissages.

Retrouvez ci-dessous :

- ► La carte des Edulab
- ► Le catalogue des formations proposées
- ► Le matériel en prêt

Plus d'information

https://pedagogie.ac-toulouse.fr/drane/edul-b

Autres Ressources

- **Cyber malveillance**
  - **se protéger :** https://www.cybermalveillance.gouv.fr/cybermenaces
  - **Signaler :** https://www.cybermalveillance.gouv.fr/diagnostic/accueil#signaler
  - **Déposer plainte :** https://www.cybermalveillance.gouv.fr/diagnostic/accueil#plainte
  - **Sensibiliser les collaborateurs :** https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-proteger-vos-donnees-en-sensibilisant-vos-collaborateurs

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

- **ANSSI**
  bonnes pratiques : https://www.ssi.gouv.fr/administration/bonnes-pratiques/
  Rançongiciel: https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf

ANSSI | Agence nationale de la sécurité des systèmes d'information

- **CNIL :** https://www.cnil.fr/
- **Déposer plainte :** https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
- **Educscol**
  - **RGPD** : https://eduscol.education.fr/398/protection-des-donnees-personnelles-et-assistance

CNIL.

éDUSCOL

Numérique éducatif : un service public partagé

Une logique de plateforme pour fédérer les acteurs

OPÉRATEURS D'ÉCOSYSTÈME LOCAL

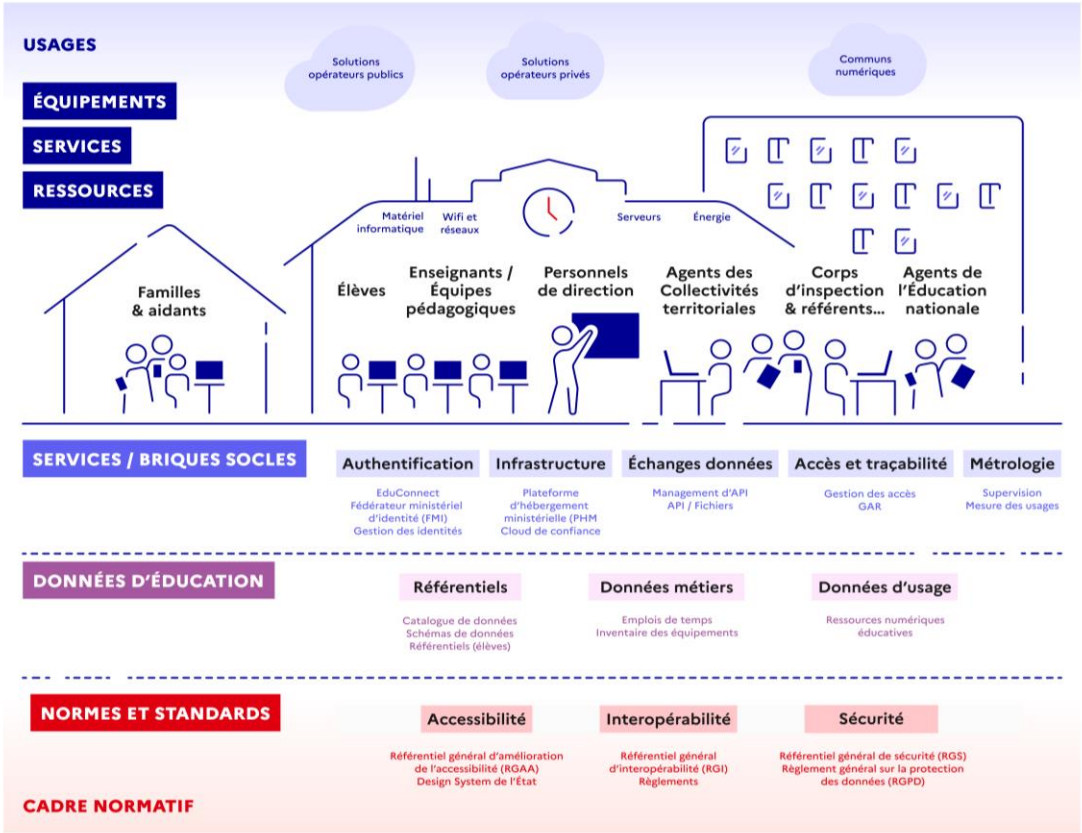
Académies / Collectivités territoriales

- Anime l'écosystème local et les communautés
- Diffuse les bonnes pratiques
- Collecte les besoins des utilisateurs
- Assure la qualité et l'adéquation de l'offre aux besoins
- Dispose des mesures d'usage

OPÉRATEUR DE L'ÉCOSYSTÈME

DNE / Académies / DGESCO

- Coordonne les communautés et fixe les règles d'interaction
- Valorise et organise l'offre
- Assure la qualité et l'adéquation de l'offre aux besoins
- Pilote la mesure des usages
- Veille sur les modèles économiques (gratuité, paiement à fourniture/à l'usage)



MANDATAIRES

Collectivités territoriales / Ministère de l'Éduc Nat / SGPI

Selon le périmètre de responsabilité :

- Veille / identifie les solutions
- Prescrit, choisit et finance les solutions, support et maintenance
- Équipe, outille et soutient les écoles et établissements

FOURNISSEURS PUBLICS & PRIVÉS

État National / Académies / Opérateurs / Entreprises Edtech

- Conçoit les solutions dans le respect du cadre commun
- Produit, exploite les données d'éducation
- Utilise les services et briques techniques socles
- Fournit et maintient les solutions
- Assure le support des solutions

AUTORITÉ DE CONCEPTION

DNE

- Consulte l'écosystème
- Fixe le cadre et les règles du jeu
- Assure l'évolutivité du cadre commun
- Accompagne les projets

Merci de votre attention.
Des questions ?