ATELIER: Cyber en toute confiance

Séminaire des Référents Numériques 2025-2026

ACADÉMIE DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Catherine MOULIN
Chargée de mission DRANE

Fiona VERCELLI
Chargée de projet TNE 38
Juriste Cyberjustice

Bruno MORAND
Chargé de mission DRANE

ACADÉMIE
DE GRENOBLE

Liberté
Égalité
Fraternité

Délégation régionale académique
au numérique éducatif

Cybersécurité

Astuces, ressources et bonnes pratiques pour protéger les données

ACADÉMIE DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Rappel des définitions

Les Etats doivent maîtriser les outils du numérique : se protéger et garantir un environnement de confiance

→ il y a une mission d'accompagnement des acteurs pour la cyber-sécurisation de leurs services

- **Cybersécurité** : vise à protéger les entreprises et citoyens contre les fraudes, arnaques, intrusions et fuites de données

- **Cyberespace** : espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques

- **Cybercriminalité** : actes utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime

Une variété d'attaques

- **Attaque par déni de service (DDoS)** : génère un trafic énorme sur un service afin d'épuiser les ressources et la bande passante d'un réseau informatique ou d'un serveur
- **Cheval de Troie** : programme donnant l'impression d'avoir une fonction utile mais qui possède une fonction cachée et potentiellement malveillante
- **Clonage de serveur DNS** : activité malveillante qui modifie un serveur DNS dans le but de rediriger un nom de domaine vers une adresse IP différente de l'adresse légitime
- **Espiogiciel – *spyware*** : logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur lequel il est installé
- **Logiciel malveillant – *malware*** : tout programme développé dans le but de nuire à un système informatique ou à un réseau
- **Rançongiciel** : forme d'extorsion imposée par un code malveillant sur un utilisateur du système
- **Réseaux de machines zombies - *Botnet*** : réseau de machines compromises à la disposition d'un individu malveillant structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines
- **Phishing** : mails piégés, ciblés et/ou massifs

ACADÉMIE DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Les acteurs de la cybersécurité

→ **ANSSI** : apporte une expertise et une assistance technique aux administrations et entreprises, sécurise les services de l'Etat et les OIV

→ **CNIL** : accompagne les particuliers à maîtriser leurs données personnelles et les professionnels dans leur mise en conformité

→ **Ministère des Armées** : code de la défense, CALID, CASSI, CRPOC et ComCyber

→ **Ministère de l'Intérieur** : garantir l'Etat de droit, défendre les intérêts de la Nation, assurer la confiance numérique des utilisateurs, assurer la prévention par la sensibilisation et par la formation, etc.

→ **Plateforme cybermalveillance.gouv.fr. (2015)** : permet aux particuliers, entreprises et collectivités d'être mis en relation avec des acteurs de proximité référencés pour les aider en cas d'attaques numériques

→ **Des plus petits acteurs** : des experts en sécurité des systèmes d'information pour conseiller les entreprises afin qu'ils se protègent au mieux + faire des audits + intervenir en cas de compromission d'un système

Au sein des entreprises : nommer un **RSSI** (Responsable de la Sécurité des Systèmes d'Information)

ACADÉMIE DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Les bonnes pratiques

La sécurité du poste de travail

· Faire les mises à jour automatiques du système d'exploitation

· Installer les logiciels de protection

· Ne pas utiliser de service « grand public » sur le terminal professionnel

· Ne pas installer de logiciels non autorisés sur les terminaux d'entreprise

· Verrouiller le poste quand on s'absente

Les équipements nomades

· Mettre en place un code d'accès, mot de passe efficace

· Appliquer toujours les dernières mises à jour de sécurité

· N'installer que des applications depuis les magasins officiels

· Eviter les réseaux Wifi public « ouverts » ou inconnus

La sauvegarde

· Définir un plan de sauvegarde et de restauration des données et de l'infrastructure

· Faire des sauvegardes régulières de son travail

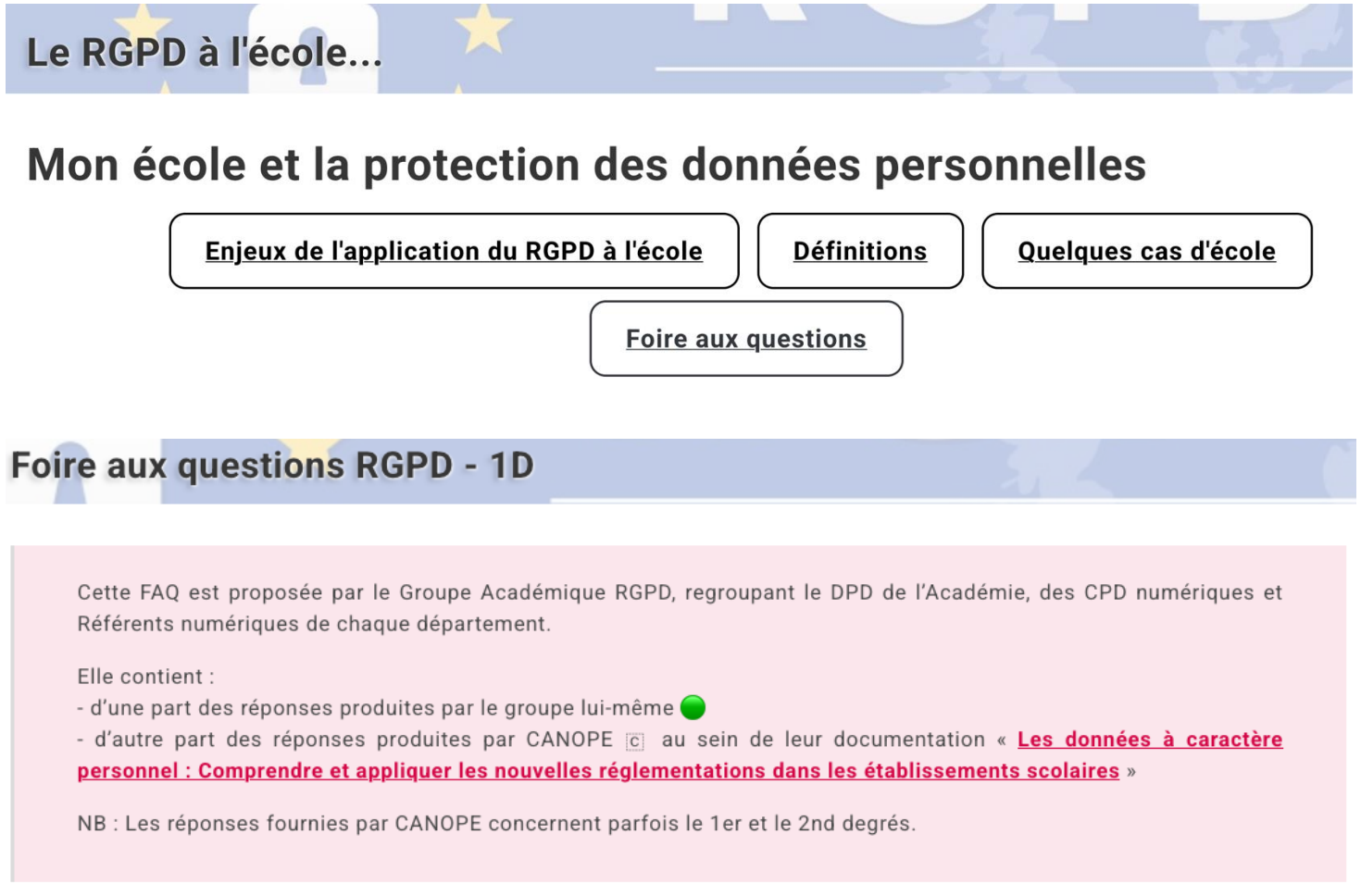
· Télécharger les fichiers sur lesquels on travaille en local

ACADÉMIE DE GRENOBLE
Liberté Égalité Fraternité

Délégation régionale académique au numérique éducatif

Des ressources

Ressources site :



ACADÉMIE DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Des ressources

Ressources site :

- https://dane.web.ac-grenoble.fr/actualites-academiques/cybersecurite-enjeux
- https://dane.web.ac-grenoble.fr/1d-0/les-concours-cyber
- Jeu L'odyssée du numérique (cartes « protection ») : https://dane.web.ac-grenoble.fr/odyssee-du-numerique
- Fini la bricole : https://dane.web.ac-grenoble.fr/reglementation-0/fini-la-bricole*

Ressources nationales :

- Le mooc de l'ANSSI : https://secnumacademie.gouv.fr/
- Règles d'utilisation du poste et conseils de navigation en ligne : https://www.cnil.fr/sites/cnil/files/2025-03/france-service-fond-d-ecran.pdf
- Conseils pour protéger sa vie numérique : https://www.cnil.fr/sites/default/files/2025-03/poster-france-service-cnil.pdf

ACADÉMIE
DE GRENOBLE

Liberté
Égalité
Fraternité

Délégation régionale académique
au numérique éducatif

Cyberharcèlement

Quiz interactif, conseils et outils pour réagir et prévenir

Cyberharcèlement

Publication d'insultes, d'injures, d'humiliations par le biais de sites internet et des réseaux sociaux, mais aussi via tout support numérique (ex : cd-rom, clé USB, disque dur, etc.).

→ Cadre légal : article 222-33-2-2 du Code pénal (harcèlement)

→ Il s'agit d'une circonstance aggravante

Cyberharcèlement scolaire

Echanges en ligne entre élèves d'un même établissement envers une victime du même établissement ou d'un autre établissement scolaire. Violences verbales, physiques ou psychologiques.

Cyberharcèlement sexuel

Ou cybersexisme.

Insultes sur son corps et/ou de rumeurs sur sa vie amoureuse, de messages à caractères sexuel ou d'humiliations répétées (via des photos/vidéos intimes, des publications de commentaires blessants).

→ Cadre légal : article 222-33 du Code pénal (harcèlement sexuel).

→ Il s'agit d'une circonstance aggravante

ACADÉMIE DE GRENOBLE
Liberté Égalité Fraternité

Délégation régionale académique au numérique éducatif

Les chiffres

Baromètre annuel sur le harcèlement et le cyberharcèlement

L'Association e-Enfance / 3018 dévoile les résultats de la 5e édition de son baromètre annuel sur le **harcèlement** et le **cyberharcèlement** (réalisée par l'Institut Audirep, avec le soutien de la Caisse d'Epargne)*.

L'étude révèle une triste réalité : le harcèlement est bien présent dans la vie des enfants et touche indifféremment toutes les catégories d'âge.

35 % des jeunes ont été touchés par le harcèlement, dès l'école primaire :

+ 11 points en seulement un an

LES CHIFFRES À RETENIR :

- **37 % des jeunes** touchés par le harcèlement ou le cyberharcèlement
- **71 % des cas de harcèlement** ont lieu au sein de l'établissement scolaire
- **25 % des victimes** ont déjà pensé à se faire du mal ou au suicide, chiffre qui monte jusqu'à 39 % chez les jeunes filles
- **41% des jeunes cyberharcelés** le sont via WhatsApp, dont 25% sur des groupes WhatsApp de classe

ACADÉMIE
DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique
au numérique éducatif

Les chiffres

18%

des enfants de 6 à 18 ans
ont été confrontés au moins une fois à du cyberharcèlement.

(Etude Association e-Enfance / 3018 et Caisse d'Epargne 2025)

ACADÉMIE
DE GRENOBLE

Liberté
Égalité
Fraternité

Délégation régionale académique
au numérique éducatif

LE CYBERHARCÈLEMENT : L'AMPLIFICATION PAR LE NUMÉRIQUE

COMMENT LE NUMÉRIQUE AGGRAVE LE HARCÈLEMENT

PUBLICATION INSTANTANÉE ET MASSIVE

Les contenus peuvent être vus par un grand nombre de personnes en quelques secondes.

AUCUN RÉPIT POUR LA VICTIME

Le harcèlement peut se poursuivre à tout moment, de jour comme de nuit, et ne laisse aucun répit pour la victime.

ANONYMAT ET SENTIMENT D'IMPUNITÉ

L'anonymat en ligne accentue le sentiment d'impunité des auteurs et la peur de parler chez les victimes.

LA COMPLICITÉ DES TÉMOINS

Les témoins deviennent complices en likant, partageant ou commentant sans réfléchir.

ACADÉMIE
DE GRENOBLE

Liberté
Égalité
Fraternité

Délégation régionale académique
au numérique éducatif

LE CYBERHARCÈLEMENT : LES DIVERSES FORMES D'ATTAQUES

COMMENT SE MANIFESTE LE CYBERHARCÈLEMENT AU QUOTIDIEN

ATTAQUES VERBALES ET RUMEURS

Messages insultants, moqueries, menaces, humiliations, incitations à la haine et fake news.

VIOLATION DE LA VIE PRIVÉE ET DES DONNÉES

Partage d'informations personnelles (photos, adresses, données privées) volées, modifiées ou détournées.

PUBLICATION ET ENVOI DE CONTENUS COMPROMETTANTS

Publication de photos/vidéos humiliantes (sextorsion, revenge porn) ou envoi de contenus pornographiques.

PIRATAGE ET USURPATION D'IDENTITÉ

Piratage de comptes ou usurpation d'identité pour tromper, insulter, ridiculiser, arnaquer, sextorsion.

ACADÉMIE
DE GRENOBLE

Liberté
Égalité
Fraternité

Délégation régionale académique
au numérique éducatif

LE CYBERHARCÈLEMENT : LES DIVERS SIGNES D'ALERTE

CERTAINS SIGNES PEUVENT ALERTER CHEZ UNE VICTIME

CHANGEMENT D'HUMEUR ET ANXIÉTÉ

Changement d'humeur, repli sur soi, anxiété inhabituelle.

ISOLEMENT ET PERTE D'INTÉRÊT

Isolement ou perte d'intérêt pour ses activités habituelles.

TROUBLES PHYSIOLOGIQUES ET ANXIÉTÉ

Troubles du sommeil ou de l'appétit, anxiété persistante.

REFUS DE L'USAGE NUMÉRIQUE

Refus soudain d'utiliser Internet, le téléphone ou les réseaux sociaux.

ACADÉMIE
DE GRENOBLE

Liberté
Égalité
Fraternité

Délégation régionale académique
au numérique éducatif

RÉFLEXES À AVOIR EN CAS DE CYBERHARCÈLEMENT

LES BONS GESTES POUR SE PROTÉGER ET AGIR

NE PAS RÉPONDRE

Évitez de vous engager dans des échanges directs. Répondre peut aggraver la situation. La première réaction peut être naturelle, mais ignorez.

CONSERVER LES PREUVES

Gardez toutes les preuves : messages, captures d'écran, emails, etc. Utiles pour signaler aux autorités et au 3018.

BLOQUER ET LIMITER L'ACCÈS

Utilisez les paramètres de confidentialité pour bloquer. Modifiez vos paramètres pour limiter l'exposition publique.

SIGNALER ET PARLER

Signalez sur la plateforme. Parlez à un proche ou contactez le 3018 3018 pour aide et suppression de contenu.

ACADÉMIE
DE GRENOBLE

Liberté
Égalité
Fraternité

Délégation régionale académique
au numérique éducatif

SI TU ES TÉMOIN, TON RÔLE EST ESSENTIEL !

NE RELAIE JAMAIS

Ne relaie jamais les moqueries, photos ou messages blessants.

SOUTIENS LA PERSONNE VISÉE

Soutiens la personne visée, même discrètement.

PRÉVIENS UN ADULTE

Préviens un adulte de confiance si la situation persiste.

DEMANDE DE L'AIDE

Et si tu ne sais pas quoi faire ou à qui en parler, demande de l'aide : tu as aussi le droit d'être écouté. Le 3018 est là pour ça.

ACADÉMIE DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Les bonnes pratiques

Flasch cards quizz

Se protéger face à l'auteur des violences :

- En parler à une personne de confiance (famille, amis, proches, enseignant, professionnel de santé, etc.)

- Signaler les contenus et leur(s) auteur(s) à la plateforme sur laquelle les contenus sont publiés, en conservant des preuves (copie écran, ou « screen »)

- Bloquer le compte du ou des auteurs des contenus violents pour ne plus voir ses contenus

- Par téléphone, tchat ou via l'application 3018, pour obtenir de l'aide de spécialistes du droit et de psychologues (gratuit 7 jours sur 7 de 9 h à 23 h)

- Exercer ses droits numériques : face à des contenus violents dévoilant des données sur soi, utiliser le droit à l'effacement

ACADÉMIE
DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique
au numérique éducatif

Les temps forts

3 temps forts de prévention tout au long de l'année :

1. Journée nationale de lutte contre le harcèlement à l'école
2. Le prix « Non au harcèlement » (limite d'envoi des productions : + serious game de Tralalere (programme Internet sans crainte)
3. Safer Internet Day

ACADÉMIE DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Les ressources

- Seriously est un projet porté par Renaissance numérique. Cette plateforme vise à pacifier les échanges sur Internet par l'intermédiaire d'exercices fondés sur l'argumentation lors des interactions entre utilisateurs. Sous forme d'ateliers, les utilisateurs sont sensibilisés aux propos haineux en ligne.
- https://www.cnil.fr/sites/default/files/2023-10/poster_cyber-reflexes2023.pdf
- https://www.cnil.fr/sites/default/files/atoms/files/affiche_gn-cnil_5_conseils_pour_proteger_sa_vie_privee.pdf
- EVARS
- Plateforme PHARE
- https://www1.ac-grenoble.fr/dispositif-de-recueil-et-de-traitement-des-signalements-des-actes-de-vdha-123728

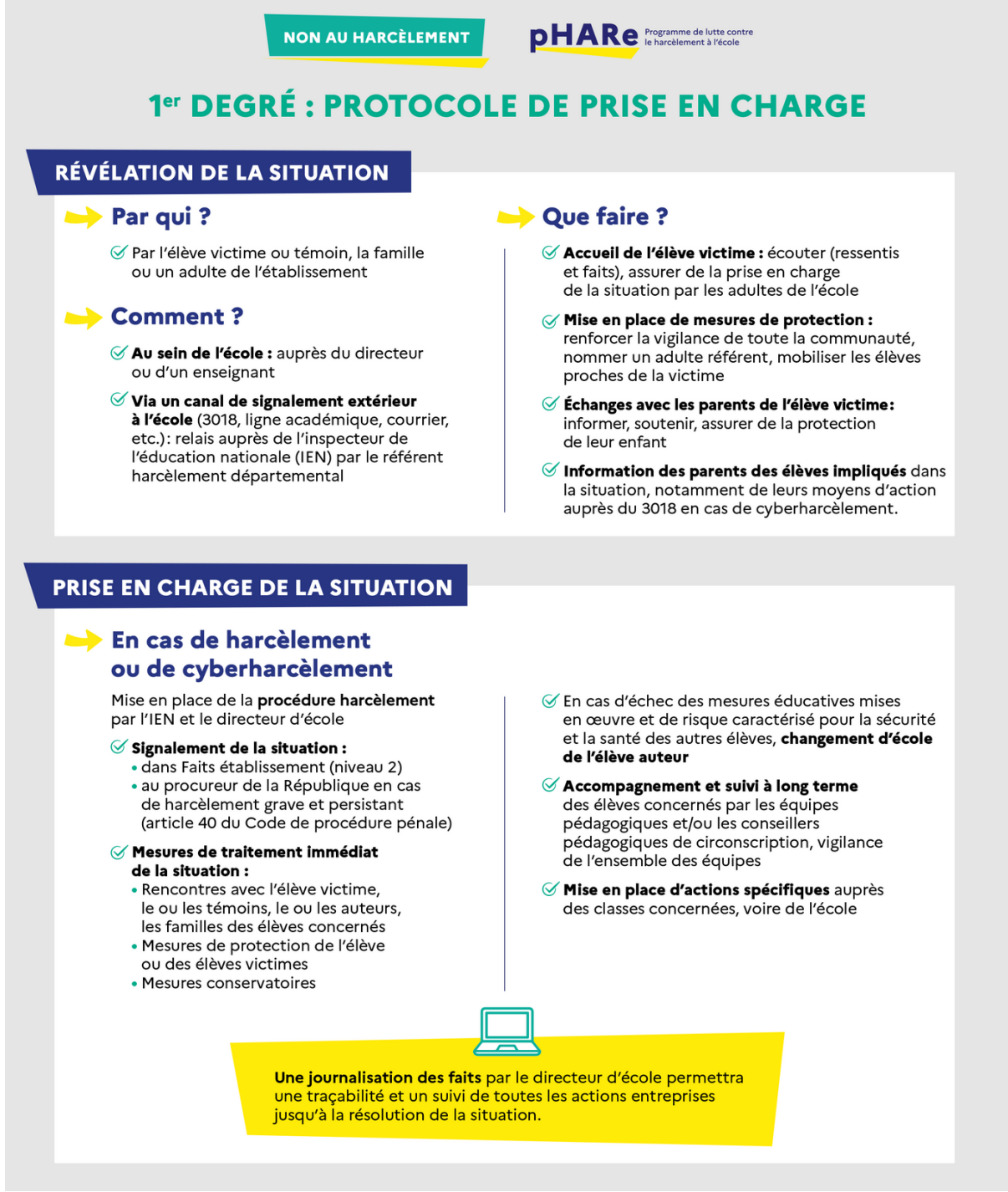
ACADÉMIE DE GRENOBLE

Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Le Dispositif pHare

[Accès au protocole complet]



NON AU HARCÈLEMENT

pHARe Programme de lutte contre le harcèlement à l'école

1er DEGRÉ : PROTOCOLE DE PRISE EN CHARGE

RÉVÉLATION DE LA SITUATION

Par qui ?

- Par l'élève victime ou témoin, la famille ou un adulte de l'établissement

Comment ?

- **Au sein de l'école :** auprès du directeur ou d'un enseignant
- **Via un canal de signalement extérieur à l'école** (3018, ligne académique, courrier, etc.): relais auprès de l'inspecteur de l'éducation nationale (IEN) par le référent harcèlement départemental

Que faire ?

- **Accueil de l'élève victime :** écouter (ressentis et faits), assurer de la prise en charge de la situation par les adultes de l'école
- **Mise en place de mesures de protection :** renforcer la vigilance de toute la communauté, nommer un adulte référent, mobiliser les élèves proches de la victime
- **Échanges avec les parents de l'élève victime:** informer, soutenir, assurer de la protection de leur enfant
- **Information des parents des élèves impliqués** dans la situation, notamment de leurs moyens d'action auprès du 3018 en cas de cyberharcèlement.

PRISE EN CHARGE DE LA SITUATION

En cas de harcèlement ou de cyberharcèlement

Mise en place de la **procédure harcèlement** par l'IEN et le directeur d'école

- **Signalement de la situation :**
  - dans Faits établissement (niveau 2)
  - au procureur de la République en cas de harcèlement grave et persistant (article 40 du Code de procédure pénale)
- **Mesures de traitement immédiat de la situation :**
  - Rencontres avec l'élève victime, le ou les témoins, le ou les auteurs, les familles des élèves concernés
  - Mesures de protection de l'élève ou des élèves victimes
  - Mesures conservatoires
- En cas d'échec des mesures éducatives mises en œuvre et de risque caractérisé pour la sécurité et la santé des autres élèves, **changement d'école de l'élève auteur**
- **Accompagnement et suivi à long terme** des élèves concernés par les équipes pédagogiques et/ou les conseillers pédagogiques de circonscription, vigilance de l'ensemble des équipes
- **Mise en place d'actions spécifiques** auprès des classes concernées, voire de l'école

Une journalisation des faits par le directeur d'école permettra une traçabilité et un suivi de toutes les actions entreprises jusqu'à la résolution de la situation.

ACADÉMIE DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Liberté d'expression et Cyberviolences

L'un des fondements de la démocratie (article 11 DDHC) : permet à chacun de dire ce qu'il pense, d'échanger des idées et de participer à la vie de la société sans avoir peur d'être sanctionné.

Mais elle n'est pas sans limite. **On ne peut pas tout dire, ni tout écrire**.

Trouver le juste équilibre entre la liberté de s'exprimer et le respect des autres est un défi important.

Une des limites : **l'incitation à la haine**

- Nature : inciter activement, via un écrit, une image, une vidéo ou tout autre support, des personnes à des réactions malveillantes et haineuses.
- Cibles : individus ou groupes en raison de caractéristiques spécifiques telles que la nationalité, la religion, l'ethnie, le sexe, l'orientation sexuelle ou le handicap.
- Caractère public :dès lors que les propos ou contenus peuvent être vus, lus ou entendus par le public.

ACADÉMIE DE GRENOBLE
Liberté
Égalité
Fraternité

Délégation régionale académique au numérique éducatif

Le blasphème : autorisé ou pas ?

En droit français, la notion de blasphème n'existe pas en tant qu'infraction pénale spécifique.

→ Conséquence directe de la laïcité et de la liberté de conscience.

Cependant, cette liberté n'est pas absolue. Limite, si l'expression constitue :

- Une diffamation ou une injure envers des personnes en raison de leur appartenance religieuse.
- Une incitation à la haine, à la violence ou à la discrimination à l'encontre de groupes religieux.
- Une atteinte à la dignité humaine.

➢ **Activité :** savoir distinguer opinion et délit