Politique d'utilisation acceptable des étudiants et entente sur la sécurité d'Internet/réseau Année scolaire 2021-2022

Les élèves signeront numériquement une version adaptée à la note de cette politique d'utilisation acceptable (AUP) et de l'Accord sur la sécurité internet/réseau à l'école par le biais d'un lien qui leurs sera fourni.

Énoncé de l'objectif - L'objectif est de fournir des appareils technologiques et l'accès à Internet et au réseau dans les écoles et à la maison pour soutenir les objectifs éducatifs du district.

Conditions de l'entente - Pour avoir accès aux systèmes informatiques scolaires, aux réseaux informatiques, aux applications logicielles, y compris Google Applications pour l'Education et à Internet, les élèves doivent lire une version de cet accord appropriée aux élèves et signer le formulaire de consentement. **Les élèves signeront numériquement le formulaire de consentement à l'école**.

Aux Parents : Veuillez lire ce document afin que vous soyez familier avec la politique des écoles publiques de Cincinnati (CPS).

Règles pour l'utilisation d'Internet/Réseau -
Le district donne accès à ses systèmes informatiques scolaires, à ses réseaux informatiques, à ses outils et appareils adoptés par le district, à ses applications logicielles, y compris Google Applications pour l'Education et à Internet à des fins éducatives seulement, y compris l'accès et le partage de l'information avec les enseignants et d'autres élèves, le stockage de dossiers, la réalisation de recherches et la collaboration sur des projets avec d'autres. Si vous avez des doutes de savoir si une activité envisagée est éducative ou non, consultez le directeur ou l'enseignant chargé de l'activité pour vous aider. L'utilisation du réseau et d'Internet du district est un privilège.
Un utilisateur qui viole cet accord doit, au minimum, avoir son accès au réseau et Internet résilié et sera soumis à des mesures disciplinaires supplémentaires en fonction de la gravité de la violation. Tous les utilisateurs sont liés par le Code de conduite des écoles publiques de Cincinnati (CPS) et les modalités suivantes:

Sécurité et éducation des élèves

La Cyber intimidation

La cyber intimidation désigne tout acte verbal ou graphique intentionnel, transmis électroniquement (y compris l'utilisation de messages texte, de messages instantanés ou d'affichage de textes ou d'images) qu'un élève ou un groupe d'élèves expose à plusieurs reprises à l'égard d'un autre élève et dont le comportement cause des dommages mentaux (y compris l'humiliation et l'embarras) et est suffisamment grave, persistant ou omniprésent.

Toute cyber intimidation, harcèlement ou intimidation est strictement interdit. Si un élève est reconnu coupable de cyber intimidation, des mesures disciplinaires seront recommandées. Si un élève pense qu'il est victime de cyber intimidation, la situation doit être immédiatement signalée à un membre du personnel adulte, comme un enseignant ou un directeur d'école. De plus, les élèves sont encouragés à aviser le personnel de l'école s'ils soupçonnent qu'un autre élève est victime de cyber intimidation.

Politique d'utilisation acceptable des étudiants et entente sur la sécurité d'Internet/réseau Année scolaire 2021-2022

Sexting

Le Sexting est l'envoi d'images sexuellement explicites par le biais de tous les médias électroniques, y compris, mais sans s'y limiter à la messagerie texte, messagerie instantanée, ou e-mail. **Le Sexting est strictement interdit** et est considéré comme une infraction de catégorie III. Le sexting doit être immédiatement signalé à un membre du personnel adulte, tel qu'un enseignant ou un directeur d'école.

Représentations de comportement interdit

- Ne jamais faire, reproduire ou distribuer des vidéos, des images, des enregistrements sonores ou d'autres supports qui montrent un comportement interdit par le Code de conduite sur la propriété de l'école ou lors d'événements scolaires, y compris à l'aide d'appareils électroniques appartenant à l'école ou personnels.
- Ne publiez jamais de représentations de comportements interdits sur des sites de réseaux sociaux tels que Facebook, Google Plus, YouTube, Instagram, Snapchat ou tout autre site Web similaire.
- Toute représentation d'un comportement interdit doit être immédiatement remise au directeur.

Réseaux sociaux/salles de chat

- Ne publiez jamais d'informations personnelles, telles que le nom complet, le numéro de sécurité sociale, l'adresse, le numéro de téléphone, les numéros de banque ou de carte de crédit, etc.
- Envisagez de ne pas poster de photos de vous-même. Ne publiez jamais de photos sensibles ou inappropriées. Si vous publiez une photo, demandez-vous s'il s'agit d'une photo que votre mère afficherait dans le salon.
- Supposons que tout ce que vous publiez est sur Internet de façon permanente.
- N'acceptez pas de rencontrer en personne quelqu'un que vous connaissez seulement à partir d'un site de réseaux sociaux l ou d'un salon de discussion.

<u>Règles de base en matière d'étiquette et de sécurité sur Internet/Réseau</u>

- Le Code de conduite des écoles publiques de Cincinnati (CPS) et les politiques du district sur le « plagiat/tricherie », « l'intimidation et d'autres formes de comportement agressif » et « L'intimidation, le harcèlement et l'intimidation — le sexting » s'appliquent à la conduite d'Internet et de réseau.
- L'application Gaggle surveillera et filtrera tous les e-mails des étudiants et le contenu de Google Apps. Les messages inappropriés seront bloqués et envoyés à un administrateur.
- Sois poli. Utilisez un langage et des graphiques appropriés.
- N'utilisez pas l'accès au réseau ou à Internet pour faire, distribuer ou redistribuer des blagues, des histoires ou d'autres documents fondés sur des insultes ou des stéréotypes liés à la race, au sexe, à l'origine ethnique, à la nationalité, à la religion ou à l'orientation sexuelle.
- Les enseignants peuvent permettre aux élèves d'utiliser le courrier électronique, les discussions électroniques, la messagerie instantanée, les sites de réseaux sociaux et d'autres formes de communications électroniques directes, y compris Gmail et Google Hangouts, à des **fins éducatives seulement** et avec une supervision adéquate.
- **Photos d'étudiants/réalisations d'étudiants** - Publier des photos d'élèves et leur travail sur des sites Web favorise l'apprentissage, la collaboration et offre l'occasion de partager les réalisations des étudiants. Les images et les réalisations des élèves de la maternelle à la 12e année ne peuvent être publiées sur le site Web que sans identifier les légendes ou les noms. Les parents/tuteurs doivent donner leur consentement par écrit pour publier la photo ou le travail scolaire de leur enfant sur n'importe quel site Web lié à l'école avant que l'article ne soit publié sur le Web.

Veuillez noter qu'en aucun cas les photos ou le travail des élèves de la maternelle à la 12e année ne seront identifiés avec des noms, des prénoms de famille sur les sites Web du district, de l'école ou des enseignants.

Le 21 Juillet 2021

Politique d'utilisation acceptable des étudiants et entente sur la sécurité d'Internet/réseau Année scolaire 2021-2022

Confidentialité - L'accès au réseau et à Internet est fourni comme un outil pour votre éducation. Le district se réserve le droit de surveiller, d'inspecter, de copier, d'examiner et de stocker à tout moment et sans préavis toute utilisation du réseau informatique et de l'accès à Internet ainsi que toute l'information transmise ou reçue dans le cadre de cette utilisation. Tous ces fichiers d'information doivent être et demeurent la propriété du district, et aucun utilisateur ne doit s'attendre à ce que ces documents lui plaise.

- **Droit d'auteur** - Tous les étudiants et professeurs doivent adhérer aux lois sur le droit d'auteur des États-Unis (P.L. 94-553) et aux Lignes directrices du Congrès qui le délimitent en ce qui concerne les logiciels, la paternité et la copie d'informations. Ne téléchargez pas de matériel ou de logiciel protégé par le droit d'auteur sans l'autorisation du propriétaire.
- Ne vendez ou n'achetez rien sur Internet.
- Ne transmettez pas ou n'accédez pas à du matériel obscène ou pornographique; aviser votre professeur si vous recevez ce matériel.
- Tout abonnement aux services de liste, aux babillards ou aux services en ligne doit être examiné par un administrateur de district et doit être approuvé par l'enseignant avant toute utilisation de ce genre.
- N'accédez pas au réseau ou à Internet par quelque moyen ou appareil autre que ceux approuvés par l'enseignant.
- Ne publiez pas de discours inapproprié sur les blogs, podcasts, applications Google ou autres outils Web 2.0.

Ces outils sont considérés comme une extension de votre salle de classe, et tout discours qui est considéré comme inapproprié dans la salle de classe est également inapproprié dans toutes les utilisations de ces outils Web. Cela comprend, sans s'y limiter, les blasphèmes et les remarques racistes, sexistes ou discriminatoires. Les commentaires faits sur les blogs seront surveillés et, s'ils sont inappropriés, supprimés. Tout étudiant qui enfreint cette règle fera l'objet de mesures disciplinaires.

- N'utilisez pas le réseau ou Internet pour toute activité illégale, y compris a) la falsification de matériel informatique, logiciel ou données, b) entrée non autorisée dans les ordinateurs et les fichiers (piratage/craquage), c) vandalisme ou destruction d'équipement bien informé, et (d) suppression de fichiers informatiques. Une telle activité est considérée comme un crime en vertu des lois étatiques et fédérales et sera disciplinée en conséquence.
- N'utilisez pas le réseau ou Internet pour envoyer des messages relatifs à des activités illégales telles que la vente ou la consommation de drogues ou d'alcool ou de quelque façon que ce soit; soutien à l'activité criminelle ou à l'activité des gangs; d'intimidation ou de harcèlement à l'adresse de toute autre personne.

Toutes les règles ci-dessus s'appliquent expressément, mais ne sont pas limitées à, l'utilisation des applications Google pour l'éducation, qui comprennent, mais ne sont pas limités à, Gmail, Google Drive, Google Calendar, Google Hangouts, Google Docs et Google Forms.

Filtrage réseau/système/contenu

- Si un problème de sécurité Internet/réseau est identifié, l'utilisateur doit en aviser un adulte, tel qu'un enseignant, qui en informera à son tour un administrateur du système.
- Le problème ne doit pas être démontré aux autres utilisateurs. ·
- N'essayez pas de vous connecter en tant qu'administrateur système. Cette action entraînera l'annulation des privilèges.·
- N'utilisez pas de proxys anonymes pour contourner le filtrage de contenu mis en œuvre par le district. · Ne chargez pas ou ne créez pas sciemment ou par inadvertance un virus informatique ou ne chargez aucun logiciel qui détruit des fichiers et des programmes, confond les utilisateurs ou perturbe les performances du système. ·

Le 21 Juillet 2021

Politique d'utilisation acceptable des étudiants et entente sur la sécurité d'Internet/réseau Année scolaire 2021-2022

- N'installez pas de logiciel tiers sans le consentement de votre administrateur désigné. ·
- Ne partagez pas vos mots de passe.
- N'utilisez pas les comptes ou mots de passe d'une autre personne. ·
- Les mesures de protection de la technologie peuvent être désactivées par une personne autorisée. Cela ne sera fait que par la gestion des technologies de l'information (ITM) pendant l'utilisation de l'ordinateur pour adultes pour permettre l'accès à Internet à des fins de recherche ou à d'autres fins légales. ·
- Ne participez pas à des activités de piratage ou de craquage ou à toute forme d'accès non autorisé à d'autres ordinateurs, réseaux ou systèmes d'information.

Si un problème de sécurité Internet/réseau est identifié, l'utilisateur doit en informer un adulte, tel qu'un enseignant, qui à son tour en informera un administrateur système. Le problème ne doit pas être démontré à d'autres utilisateurs.

Responsabilités du Professeur

- Fournira des conseils adaptés au développement des élèves qui utilisent les ressources en télécommunications et en information électronique pour mener des recherches et d'autres études liées au programme d'études du district.
- Tous les élèves seront informés de leurs droits et responsabilités en tant qu'utilisateurs du réseau du district avant d'avoir accès à ce réseau, soit en tant qu'utilisateur individuel, soit en tant que membre d'une classe ou d'un groupe
- L'utilisation des ressources en réseau servira à appuyer les objectifs éducatifs.
- Traiter les infractions commises par les élèves de cette AUP conformément au Code de conduite des écoles publiques de Cincinnati (CPS).
- Offrir d'autres activités aux étudiants qui n'ont pas de privilèges réseau et Internet.

Responsabilités du Directeur

- Inclure cette Application de code de conduite (AUP) dans le manuel des élèves de son école.
- distribuent des manuels d'étudiants à tous les élèves.
- Traiter les infractions commises par les élèves de cette application (AUP) conformément au Code de conduite des écoles publiques de Cincinnati (CPS).
- Conserver les formulaires de consentement signés au dossier pendant un an.
- Identifier au personnel enseignant les élèves qui n'ont pas la permission d'utiliser Internet.

Responsabilités du District

- S'assure r que le logiciel de filtrage et /blocage est utilisé pour bloquer l'accès à des sites et des matériaux qui sont inappropriés, offensants, obscènes, contiennent de la pornographie ou qui sont autrement préjudiciables aux mineurs.
- Restreindre la divulgation, l'utilisation et la diffusion non autorisées de renseignements personnels concernant des mineurs.
- Publier cette application code de conduite (AUP) sur le site Web du district.

Pour le support technique, veuillez contacter le Centre de support technique familial: 513-363-0688

Les écoles publiques de Cincinnati se réservent le droit de changer cette politique à tout moment.

Le 21 Juillet 2021