



Politique d'utilisation acceptable de la technologie et du réseau par les élèves et le personnel

I. OBJECTIF ET PORTÉE

Les Écoles publiques de DC (DCPS) offrent aux élèves et au personnel un accès à Internet, aux données et aux systèmes de réseau (réseau de DCPS). DCPS permet également aux élèves et au personnel d'accéder à des ordinateurs, à des tablettes, à des appareils et à d'autres technologies, comme des imprimantes (appareils ou technologie de DCPS). Le réseau et la technologie de DCPS sont fournis au personnel à des fins de planification, d'enseignement et d'administration, et aux élèves à des fins d'éducation, de recherche et de développement de carrière. La présente politique vise à :

- Établir les normes d'utilisation acceptable du réseau et de la technologie de DCPS ;
- Définir les attentes concernant l'utilisation responsable de l'intelligence artificielle ;
- Empêcher l'utilisation non autorisée et illégale du réseau et de la technologie de DCPS ;
- Se conformer à la Children's Internet Protection Act de 2000 (CIPA), à la Children's Online Privacy Protection Act (COPPA), à la Protecting Students Digital Privacy Act et à toutes les autres lois, réglementations, politiques et procédures applicables.

La présente politique s'applique à tous les élèves, membres du personnel, visiteurs et autres personnes qui utilisent le réseau ou les appareils de DCPS, et annule la précédente Politique d'utilisation acceptable de la technologie et du réseau par les élèves et le personnel de DCPS (2021).

II. POUVOIRS ET DROIT APPLICABLE¹

Source	Citation
Droit fédéral	- Children's Internet Protection Act (CIPA), codifiée à 47 U.S.C. § 254(h)(5) - Children's Online Privacy Protection Act de 1998, codifiée à 15 U.S.C. § 6501 <i>et seq.</i> - Neighborhood Children's Internet Protection Act, codifiée à 47 U.S.C. § 254(l)
Règlements fédéraux	- Children's Online Privacy Protection Rule, 16 C.F.R. Partie 312
Droit du District de Columbia	- Protecting Students Digital Privacy Act de 2016, D.C. Law 21-218, codifiée à D.C. Official Code 38-831.01 <i>et seq.</i>
Règlements municipaux du District de Columbia	- 5-B DCMR § 2500 <i>et seq.</i> – Student Discipline - 6-B DCMR § 1610 – Employee Progressive Discipline

¹ Rien dans la présente politique ne prévaut sur le droit fédéral, étatique ou local.

III. TERMES ET DÉFINITIONS CLÉS

Intelligence artificielle (IA) désigne une branche de l'informatique traitant de la simulation de comportements intelligents dans les ordinateurs.

Réseau de DCPS désigne les systèmes Internet, de données et de réseau fournis par DCPS à tous les élèves et membres du personnel de DCPS.

Personnel de DCPS désigne tous les employés (à temps plein ou à temps partiel), sous-traitants, mandataires, représentants, bénévoles de DCPS ou toute autre personne agissant au nom de DCPS qui ont accès au réseau et à la technologie de DCPS.

Technologie de DCPS désigne les ordinateurs, tablettes, appareils et autres technologies fournis par DCPS aux élèves et au personnel.

Expulsion désigne le retrait d'un élève de l'école où il est inscrit pour des raisons disciplinaires pour le reste de l'année scolaire ou plus, conformément à la politique de l'agence locale d'éducation.

Renseignements personnels désigne les renseignements qui, lorsqu'ils sont utilisés seuls ou en combinaison avec d'autres données pertinentes, peuvent permettre d'identifier une personne. Les renseignements personnels comprennent, sans toutefois s'y limiter, le nom complet, l'adresse du domicile ou une autre adresse physique, le pseudo ou le nom d'utilisateur lorsqu'il est utilisé comme coordonnées en ligne, et un fichier photo, audio ou vidéo contenant l'image ou la voix d'une personne.

Mesures disciplinaires progressives désigne un système disciplinaire visant les employés, qui fournit une gamme graduée de mesures pour répondre aux problèmes de performance ou de conduite des employés. Les mesures disciplinaires progressives de DCPS comprennent des conseils verbaux, des avertissements, des réprimandes et des mesures défavorables.

Suspension désigne le retrait temporaire d'un élève des cours qu'il suit normalement dans le cadre de son emploi du temps à titre de mesure disciplinaire. Pendant sa suspension, soit l'élève reste à l'école sous la surveillance du personnel scolaire, soit il n'est pas autorisé à venir à l'école.

IV. EXIGENCES

A. Généralités

DCPS fournit le réseau et la technologie de DCPS au personnel et aux élèves et les autorise à les utiliser. En fournissant des ressources technologiques et en autorisant leur utilisation, DCPS ne renonce pas à la propriété ou au contrôle de la technologie et du matériel des systèmes fournis par DCPS. Sauf indication contraire ci-dessous, il n'y a aucune attente de confidentialité à avoir concernant les informations stockées dans les systèmes de DCPS ou transmises sur le réseau de DCPS, et DCPS se réserve le droit de consulter, d'examiner, de copier, de stocker ou de supprimer tous les fichiers stockés sur la technologie de DCPS ou dans les comptes du réseau de DCPS, ainsi que toutes les communications utilisant le réseau de DCPS. Les messages et fichiers électroniques stockés sur les ordinateurs de DCPS ou transmis à l'aide

des systèmes de DCPS peuvent être traités comme n'importe quel autre bien de l'école. Le personnel de DCPS peut examiner les fichiers et les messages pour mener des enquêtes, se conformer aux exigences légales, maintenir l'intégrité du système et, si nécessaire, s'assurer que les utilisateurs de la technologie et du réseau agissent de manière responsable et conformément à la présente politique. Tous les comptes créés par DCPS pour les élèves ou le personnel peuvent être surveillés par DCPS.

1. Élèves

DCPS fournira un avis de cette politique lors du processus d'inscription annuel, et tous les parents et élèves majeurs seront invités à en accuser réception. Les élèves et les parents peuvent être tenus de signer un Accord d'utilisation responsable de la technologie et du réseau par l'élève (Accord d'utilisation responsable par l'élève), inclus dans les annexes et disponible sur le site Web de DCPS. L'Accord d'utilisation responsable par l'élève décrit l'utilisation responsable et les activités interdites pour les élèves qui utilisent la technologie de DCPS ou accèdent au réseau de DCPS. Les écoles peuvent également exiger que les élèves et les parents signent des accords propres à l'école, qui détaillent les processus d'emprunt et de retour de la technologie, désignent le personnel scolaire ayant des rôles spécifiques liés à la technologie et établir des règles propres à l'école.

DCPS offre aux élèves des cours annuels sur la citoyenneté numérique et la sécurité en ligne. Les élèves doivent suivre les cours dans le Centre des élèves sur la citoyenneté et la culture numériques², y compris le module sur l'utilisation des appareils et la façon d'en prendre soin, et l'achèvement d'un cours peut être requis pour qu'un élève reçoive un appareil ou un compte de DCPS.

Le non-respect de ces règles sera traité dans le cadre des règlements et politiques disciplinaires de DCPS, y compris la Politique sur les écoles sûres et positives³, et peut entraîner une perte d'accès au réseau ou à la technologie de DCPS pendant des périodes croissantes, à condition que les élèves puissent participer aux cours et faire leurs devoirs par d'autres moyens et soient en mesure de recevoir tous les services nécessaires d'éducation spécialisée et d'apprentissage de l'anglais. Dans certains cas, une inconduite peut également constituer une infraction pénale.

2. Personnel

DCPS informera le nouveau personnel de la présente politique au cours du processus d'intégration, et l'Accord d'utilisation responsable de la technologie par le personnel (Accord d'utilisation responsable par le personnel) inclus dans les annexes sera disponible sur le site Web de DCPS à titre de référence supplémentaire et permanente. Le personnel à qui un appareil de DCPS a été attribué peut également être invité à signer ou à signer de nouveau un formulaire d'accusé de réception de l'Accord d'utilisation responsable de la technologie par le personnel au moment de recevoir son appareil ou avant.

Le gouvernement de DC, le Bureau du directeur de la technologie de DC (OCTO) ou DCPS peuvent exiger que le personnel suive une formation liée à la cybersécurité ou à des sujets connexes. Le personnel qui ne suit pas ces formations dans les délais impartis ou qui ne respecte pas la présente politique peut faire l'objet de mesures disciplinaires progressives.

² Disponible sur <https://dcps.instructure.com/enroll/Y8Y7KY>.

³ Disponible sur <https://dcps.dc.gov/page/dcps-policies>.

B. Réseau, courrier électronique et applications

1. Réseau

Le réseau et la technologie de DCPS sont fournis au personnel à des fins de planification, d'enseignement et d'administration, et aux élèves à des fins d'éducation, de recherche et de développement de carrière. Le réseau de DCPS fournit au personnel et aux élèves un accès interne aux informations et ressources de DCPS, et aux applications approuvées par DCPS, et un accès externe à Internet. L'accès au réseau de DCPS, y compris à Internet, est fourni aux élèves uniquement pour soutenir leur éducation, leur recherche et leur développement de carrière. L'utilisation du réseau de DCPS est un privilège. Le personnel et les élèves qui enfreignent toute partie de la présente politique ou de politiques connexes peuvent faire l'objet de l'annulation de leurs privilèges d'utilisation du réseau de DCPS et d'éventuelles mesures disciplinaires.

L'accès au réseau et la bande passante du réseau sont fournis aux écoles pour assurer les services scolaires et opérationnels. DCPS se réserve le droit d'établir des priorités dans l'utilisation de la bande passante du réseau et de limiter certaines activités du réseau qui ont un impact négatif sur les services scolaires et opérationnels. Il est interdit aux utilisateurs du réseau d'utiliser le réseau de DCPS pour accéder à des contenus jugés inappropriés ou illégaux, y compris, mais sans s'y limiter, des contenus pornographiques, obscènes, illégaux ou incitant à la violence.

DCPS ne garantit pas que le fonctionnement ou la qualité des services réseau fournis seront exempts d'erreurs ou de défauts. DCPS n'est pas responsable des demandes, pertes, dommages, coûts ou autres obligations découlant de l'utilisation du réseau ou des comptes. Tous les frais engagés par une personne en raison de l'utilisation du réseau seront à sa charge exclusive. DCPS n'est pas responsable de l'exactitude ou de la qualité des informations obtenues en utilisant le système, à moins que les informations ne soient un contenu produit par DCPS. Toute déclaration non produite par DCPS et accessible sur le réseau ou sur Internet est considérée comme étant le point de vue individuel de l'auteur et non celui de DCPS, du gouvernement du District de Columbia, de leurs affiliés ou de leurs employés.

2. Filtres et surveillance

Comme l'exige la Children's Internet Protection Act (CIPA), DCPS est tenu de protéger les élèves contre les menaces en ligne et de les informer à ce sujet, de bloquer l'accès aux contenus inappropriés et de surveiller l'utilisation d'Internet par les mineurs sur les réseaux scolaires⁴.

DCPS utilise une technologie de protection pour bloquer ou filtrer l'accès aux représentations visuelles obscènes, pornographiques ou préjudiciables aux mineurs sur Internet. Sauf dans les cas décrits dans la section IV.F ci-dessous, DCPS se réserve le droit de superviser et de surveiller les activités en ligne des élèves et de consulter, d'examiner, de copier, de stocker ou de supprimer toute information ou fichier électronique, ainsi que de les communiquer à des tiers s'il le juge nécessaire. Les élèves n'ont aucune attente de confidentialité à avoir concernant l'utilisation des biens de DCPS, du réseau informatique de DCPS, d'Internet, des fichiers ou du courrier électronique lorsqu'ils sont à l'intérieur du réseau, sauf dans les cas établis par la Protecting Students Digital Privacy Act (voir la section IV.F ci-dessous).

⁴ 47 U.S.C. 254(h)(5)(B).

DCPS utilise également un système de gestion de la sécurité pour analyser et examiner le contenu trouvé dans les fichiers des élèves stockés en ligne, les e-mails entrants et sortants de DCPS, les pièces jointes des e-mails de DCPS et les liens vers des sites Web. Ce système bloque les contenus et les images potentiellement dangereux et informe le personnel de DCPS en cas d'urgence, comme en cas de menace ou de violence envers soi-même ou envers autrui.

3. Applications

En vertu de la Children's Online Privacy Protection Act (COPPA), les exploitants de sites Web ou de services en ligne destinés aux enfants de moins de 13 ans, ainsi que les exploitants d'autres sites Web ou services en ligne qui savent qu'ils collectent des renseignements personnels en ligne concernant un enfant de moins de 13 ans, doivent obtenir le consentement vérifiable des parents avant de collecter, d'utiliser ou de communiquer des renseignements personnels concernant des enfants⁵.

Lorsque DCPS passe un contrat avec un site Web ou un service en ligne pour collecter des renseignements personnels aux fins de leur utilisation par DCPS et au bénéfice de DCPS, et à aucune autre fin commerciale, l'exploitant peut obtenir le consentement de DCPS et n'est pas tenu d'obtenir le consentement directement auprès des parents⁶. DCPS fournira aux parents un avis du consentement fourni par DCPS au moyen d'une liste électronique, publiée sur le site Web de DCPS, de tous les sites Web et services en ligne conformes à la COPPA avec lesquels DCPS passe des contrats ou auxquels les élèves de moins de 13 ans doivent accéder, y compris un lien vers la politique de confidentialité de chaque exploitant, et le processus à suivre par les parents pour refuser la collecte de renseignements personnels. Le personnel du DCPS n'est pas autorisé à exiger des élèves de moins de 13 ans qu'ils accèdent à des sites et services non conformes à la COPPA ou à des sites et services conformes à la COPPA lorsque les parents ont choisi de refuser la collecte de renseignements personnels.

4. Contrôle d'accès

DCPS met en œuvre des mesures de contrôle d'accès de sécurité pour garantir un accès approprié au réseau et à la technologie pour tous les utilisateurs et prévenir les accès non autorisés et les menaces potentielles. DCPS attribue l'accès des utilisateurs au réseau de DCPS, aux comptes de messagerie de DCPS et aux applications autorisées par DCPS en fonction du niveau scolaire ou de la demande de l'école ou de l'enseignant, comme suit :

- **Accès** : Tous les élèves et le personnel doivent utiliser leurs informations d'identification et mots de passe personnalisés pour se connecter aux systèmes et appareils de DCPS.
- **E-mail** : À partir de la 9^e année, les élèves reçoivent des comptes de messagerie de DCPS après avoir suivi avec succès un cours sur la citoyenneté numérique. Les élèves des autres classes peuvent recevoir des comptes de messagerie de DCPS après avoir suivi un cours sur la citoyenneté numérique, à la discrétion du personnel du DCPS. Pour suivre le cours sur la citoyenneté numérique, les élèves ayant certains handicaps devraient avoir accès aux

⁵ Voir 16 C.F.R. Partie 312.5. Cette exigence s'applique également à tout changement important dans les pratiques de collecte, d'utilisation ou de communication auxquelles un parent a préalablement consenti. Les exploitants doivent également donner aux parents la possibilité de consentir à la collecte et à l'utilisation des renseignements personnels de l'enfant sans consentir à leur communication à des tiers.

⁶ Pour plus d'informations sur la conformité à la COPPA, veuillez consulter

<https://www.ftc.gov/tipsadvice/business-center/guidance/complying-coppa-frequently-asked-questions>.

aménagements en classe et pour les examens prévus dans leur IEP. Ceux-ci peuvent comprendre la lecture à haute voix et la répétition des instructions, l'amélioration de la lisibilité du texte, la simplification du contenu et d'autres mesures.

- **Applications** : DCPS donne accès à un ensemble standard d'applications approuvées pour tout le personnel et les élèves de DCPS. L'accès du personnel est accordé en fonction des responsabilités professionnelles et, pour certaines applications, en fonction de la demande du chef d'établissement. Les élèves ont accès à un ensemble d'applications approuvées. Les élèves peuvent avoir accès à d'autres applications au-delà de celles approuvées à la demande de l'école et de l'enseignant.
- **Élèves diplômés ou qui partent** : Les élèves qui obtiennent leur diplôme ou quittent DCPS n'auront plus accès à la technologie ou aux systèmes de DCPS, y compris les applications et les documents stockés.

5. Mots de passe

La protection par mot de passe est requise sur toutes les technologies délivrées par DCPS afin d'empêcher leur utilisation par toute personne non autorisée par DCPS. Les utilisateurs sont tenus de respecter les exigences en matière de mot de passe de DCPS lorsqu'ils se connectent aux ordinateurs, réseaux et systèmes en ligne de l'école. Les utilisateurs seront automatiquement invités à répondre aux exigences en matière de mot de passe de DCPS dans le cadre du processus de mise à jour régulière de leur mot de passe.

Les élèves et le personnel ne sont pas autorisés à partager leur mot de passe ou le mot de passe de tout autre élève ou membre du personnel de DCPS qu'ils pourraient connaître, que ce soit innocemment ou en violation de la présente politique, et doivent faire preuve d'une vigilance accrue pour éviter les tentatives de fraude par e-mail qui demandent des mots de passe ou d'autres renseignements personnels. DCPS demande aux élèves de participer à des cours sur la citoyenneté numérique et la sécurité en ligne afin d'apprendre la façon d'éviter ces tentatives de fraude et d'autres bonnes pratiques pour une utilisation sûre de la technologie.

Les élèves handicapés qui ne sont pas en mesure de maîtriser les cours sur la citoyenneté numérique ne sont pas visés par ces exigences en matière de mot de passe.

Les sanctions pour l'utilisation interdite de mots de passe peuvent entraîner des restrictions d'accès au réseau ou l'annulation de comptes. De plus, les infractions peuvent entraîner des mesures disciplinaires ou des actions en justice à l'encontre des élèves, notamment la suspension, l'expulsion et des poursuites pénales.

6. Accès à la télésanté/télémedecine

Le personnel et les élèves de DCPS sont autorisés à accéder aux séances de télésanté sur les appareils de DCPS. Bien que DCPS n'ait pas l'intention de surveiller activement les séances de télésanté, la loi fédérale exige que les districts scolaires analysent les données et surveillent l'activité des élèves sur les appareils fournis par l'école, ce qui pourrait inclure les dossiers médicaux ou d'autres documents enregistrés sur les disques durs des appareils. Les séances de télésanté en direct ne seront pas surveillées. Si des données confidentielles sont stockées sur les disques durs des appareils, elles seront effacées lorsque du retour des appareils dans les stocks.

7. Vidéoconférence

Il y a vidéoconférence lorsque le personnel de DCPS et les élèves communiquent entre eux en temps réel, par le son et l'image, à l'aide d'une application de vidéoconférence. Les enseignants et le personnel peuvent enregistrer la vidéoconférence pour que les élèves et eux-mêmes puissent la consulter ultérieurement.

Le personnel ne doit pas communiquer de renseignements personnels identifiables concernant les élèves lors des séances de vidéoconférence.

Le personnel et les élèves doivent signaler tout comportement inapproprié ou préoccupant pouvant survenir pendant une vidéoconférence au Bureau de l'intégrité de DCPS⁷. Le personnel et les élèves doivent continuer à suivre la Politique sur les droits et responsabilités des employés de DCPS⁸, la Politique sur les réseaux sociaux⁹ et toute autre politique, réglementation et loi applicable concernant les interactions entre le personnel et les élèves.

8. Intelligence artificielle (IA)

Comme pour toute technologie, les élèves et le personnel sont tenus d'utiliser l'IA de manière responsable et éthique. Les outils d'IA doivent être utilisés par les élèves et le personnel comme un complément, et non comme un substitut, à l'apprentissage. DCPS offrira aux élèves des leçons sur les avantages et les risques de l'IA dans des cours sur la citoyenneté numérique et des cours axés sur l'IA.

Bien que d'autres parties de cette politique abordent la question, les utilisations suivantes de l'IA sont spécifiquement interdites et feront l'objet d'un examen supplémentaire :

- Intimidation et harcèlement : Il est interdit aux élèves d'utiliser l'IA d'une manière qui pourrait nuire à eux-mêmes ou à autrui. L'utilisation d'outils d'IA pour manipuler des médias afin de se faire passer pour autrui est interdite.
- Plagiat et tricherie : Il est interdit aux élèves de présenter un travail généré par l'IA comme leur travail original ou d'utiliser l'IA pour répondre à des questions d'évaluation, d'examen ou d'autres devoirs (sauf indication contraire de leur enseignant).

Conformément à la Politique sur les écoles sûres et positives de DCPS¹⁰, le personnel doit prendre des mesures disciplinaires, en commençant par la mesure appropriée la moins sévère dans la gamme des mesures disciplinaires autorisées. Cette gamme peut aller de la possibilité de présenter un nouveau travail à une réduction de la note.

a. Considérations supplémentaires concernant l'utilisation de l'IA par le

⁷ Pour contacter le Bureau de l'intégrité, remplir le formulaire de référence en ligne, disponible sur <https://dcps.dc.gov/page/office-integrity> ou envoyer un e-mail à dcps.cio@k12.dc.gov.

⁸ Disponible sur <https://dcps.dc.gov/page/dcps-policies>.

⁹ Disponible sur <https://dcps.dc.gov/page/dcps-policies>.

¹⁰ Disponible sur <https://dcps.dc.gov/publication/safe-and-positive-schools-policy>.

personnel

DCPS tient à jour une liste d'outils améliorés par l'IA approuvés pour l'apprentissage des élèves et fournira des séances de formation professionnelle pour soutenir le déploiement approprié de ces outils. Si les enseignants et les chefs d'établissement souhaitent utiliser un outil d'IA qui ne figure pas sur la liste établie par l'équipe de technologies de l'éducation de DCPS, cet outil doit répondre aux critères définis par l'équipe de technologies de l'éducation et ils doivent soumettre le formulaire d'approbation d'outil d'IA avant de l'acheter et de l'utiliser en classe ou pour un devoir. Ces critères et le formulaire sont disponibles sur le site Web SharePoint des technologies de l'éducation : <https://dck12.sharepoint.com/sites/DCPSEdTechInformationResources>.

Le personnel est tenu de vérifier l'exactitude de tout contenu produit par l'IA en utilisant des sources fiables, car le contenu généré par l'IA peut contenir des erreurs ou des préjugés. Lorsqu'il utilise l'IA pour les communications, comme la rédaction d'e-mails destinés aux parents, le personnel doit s'assurer que le langage est professionnel et exempt d'inexactitudes et de préjugés. Le personnel doit examiner tout le contenu généré par l'IA et l'analyser de manière critique avant de l'utiliser.

C. Technologie (y compris les ordinateurs, les ordinateurs portables et les tablettes)

1. Soutien des appareils

DCPS fournit un soutien de base de la technologie de DCPS en matière d'installation, de synchronisation et de logiciels. Les appareils doivent être connectés régulièrement au réseau de DCPS pour recevoir des mises à jour logicielles ou à des fins d'inventaire. Une protection par mot de passe est requise sur toute technologie délivrée par DCPS pour empêcher l'utilisation non autorisée en cas de perte ou de vol.

2. Dommages, perte ou vol

Le personnel doit prendre soin de la technologie de DCPS et peut être tenu financièrement responsable en cas de dommages, de perte ou de vol de biens dus à la négligence. Les exemples de négligence comprennent, sans s'y limiter :

- Dommages résultant du fait de laisser la technologie de DCPS dans un véhicule ou dans un autre endroit exposé à la chaleur, au froid ou à l'humidité ;
- Dommages dus à des boissons ou de la nourriture renversées ;
- Vol résultant du fait de laisser la technologie de DCPS sans surveillance ou dans un endroit non sécurisé.

Un membre du personnel de DCPS ne doit utiliser que l'appareil qui lui a été attribué par l'équipe informatique de DCPS et il lui est interdit de prendre ou d'utiliser des appareils attribués à d'autres employés actuels ou passés.

Les élèves doivent prendre des mesures raisonnables pour éviter qu'un appareil ne soit endommagé, perdu ou volé. Si l'appareil d'un élève est endommagé, le personnel de DCPS de l'école de l'élève peut enquêter pour déterminer si les dommages causés à l'appareil résultent d'une négligence ou d'actes intentionnels de vandalisme. Cette enquête doit prendre en compte les facteurs qui ont une incidence sur la capacité de l'élève à comprendre la manière appropriée de prendre soin de l'appareil, notamment son âge et tout handicap pertinent. Les exemples de dommages résultant *d'une négligence ou d'actes*

intentionnels de vandalisme comprennent, sans s'y limiter :

- Dessiner sur l'appareil à l'aide d'un marqueur permanent, graver des mots/dessins à l'aide d'un objet pointu, ou présence de marques de morsures d'animaux sur l'appareil ;
- Dommages à plusieurs endroits dus à une mauvaise manipulation ou à un manque de soin de l'appareil (par exemple, l'écran est fissuré, le clavier est endommagé, il manque des touches, le boîtier extérieur de l'ordinateur portable montre des signes d'impact à plusieurs endroits ou l'ordinateur portable/la tablette est retourné en plusieurs morceaux) ;
- Dommages causés par une force excessive, dommages causés par un impact avec des objets pointus ou durs, ou dommages causés par l'enfoncement d'objets dans les ports USB ou d'alimentation de l'ordinateur portable ;
- L'appareil a été complètement immergé dans l'eau ou dans d'autres liquides ;
- Dommages répétés si l'élève a endommagé trois (3) appareils ou plus au cours d'une année scolaire.

Les mesures disciplinaires à l'encontre des élèves en cas de dommages à des appareils résultant d'une négligence ou d'actes intentionnels de vandalisme seront déterminées dans le cadre de la Politique sur les écoles sûres et positives de DCPS¹¹, des règlements disciplinaires et de la loi, ainsi que de la présente politique d'utilisation acceptable.

Les élèves ne pourront pas être pénalisés pour des dommages résultant de l'usure normale ou d'accidents involontaires. Les exemples de dommages aux appareils résultant de *l'usure normale* comprennent, sans s'y limiter :

- Touches manquantes sur le clavier ;
- Écran fissuré à cause de chutes accidentelles ;
- Dommages isolés sur une petite partie de l'appareil, tels que les coins/côtés de l'écran, qui pourraient être le résultat de chutes accidentelles ;
- Déversements accidentels de liquide sur le clavier ;
- Dommages causés par une surtension.

Si la technologie de DCPS est perdue, volée ou endommagée, les élèves doivent en informer un enseignant ou le chef d'établissement ; les membres du personnel doivent informer leur superviseur et un point de contact de la technologie de DCPS. DCPS prendra toutes les mesures raisonnables pour récupérer les biens perdus et assurer la sécurité de toute information contenue sur l'appareil. DCPS peut choisir de déployer un logiciel de géolocalisation sur les appareils pour localiser les appareils perdus ou volés ou désactiver à distance les appareils qui ne sont pas retournés sur demande. Les appareils endommagés doivent être retournés à l'équipe informatique de DCPS (AssetAdmin@k12.dc.gov) et ne doivent pas être éliminés par les élèves, les familles ou le personnel. L'appareil doit d'abord être évalué par l'équipe informatique de DCPS et le Bureau du directeur de la technologie de DC avant d'être remplacé.

¹¹ Disponible sur <https://dcps.dc.gov/page/dcps-policies>.

3. Utilisation à la maison ou jusqu'au lendemain par les élèves

Le personnel scolaire de DCPS peut fournir aux élèves des appareils de DCPS pour les utiliser à la maison ou jusqu'au lendemain, à la discrétion du chef d'établissement ou de l'équipe de l'IEP, s'il y a lieu et conformément à la présente politique. Les élèves de DCPS et un parent/tuteur doivent signer l'Accord d'utilisation acceptable par l'élève ci-joint (voir les annexes) avant de se voir attribuer et de recevoir un appareil pour l'utiliser à domicile ou jusqu'au lendemain. Le personnel scolaire de DCPS doit respecter les exigences en matière de confidentialité en vertu de la Protection of Student Digital Privacy Act, et les parents et les élèves doivent être conscients que ces appareils peuvent être surveillés et accessibles par le personnel de DCPS¹².

L'élève peut emporter la technologie d'assistance à la maison, si l'équipe de l'IEP de l'élève, en collaboration avec l'équipe de la technologie d'assistance de DCPS, détermine que l'élève a besoin de ces aides pour accomplir des tâches éducatives à la maison (par exemple, devoirs, communication). Les élèves doivent suivre toutes les politiques de DCPS concernant l'utilisation de cette technologie à la maison, tout comme ils le feraient s'ils utilisaient la technologie à l'école. Pour plus d'informations sur la technologie d'assistance, veuillez consulter le site Web sur la technologie d'assistance de DCPS¹³ ou contacter DCPS.AssistiveTech@k12.dc.gov ou l'équipe de l'IEP de l'élève.

D. Conduite et utilisation acceptable

En utilisant le réseau et la technologie de DCPS, le personnel et les élèves acceptent de suivre toutes les réglementations, politiques et lignes directrices pertinentes du gouvernement de DC, du Bureau du directeur de la technologie de DC et de DCPS. Le personnel et les élèves doivent signaler toute utilisation abusive ou violation des protocoles aux enseignants, aux superviseurs appropriés, aux administrateurs ou aux employés des Services centraux dès qu'ils en ont connaissance¹⁴.

Le personnel et les élèves ne doivent pas utiliser le réseau ou la technologie de DCPS, y compris l'accès à Internet, à l'intranet, aux outils de collaboration, aux outils de communication en masse, aux réseaux sociaux ou au courrier électronique, pour utiliser, enregistrer, partager, télécharger, publier, envoyer par courrier, afficher, stocker, ou transmettre de quelque manière que ce soit tout contenu, communication ou information qui :

1. Est haineux, harcelant, menaçant, calomnieux ou diffamatoire ;
2. Est offensant ou discriminatoire envers des personnes en raison de la race, de la couleur, de la religion, de l'origine nationale, du sexe, de l'âge, de l'état matrimonial, de l'apparence personnelle, de l'orientation sexuelle, de l'identité ou de l'expression de genre, de la situation familiale, des responsabilités familiales, de l'inscription, de l'affiliation politique, des informations génétiques, du handicap, de la source de revenus, du statut de victime d'une infraction intrafamiliale, du lieu de résidence ou d'affaires, ou du statut de victime ou de membre de la famille d'une victime de violence familiale, d'infraction sexuelle ou de harcèlement ;
3. Constitue ou favorise une infraction pénale ou donne lieu à une responsabilité civile en vertu de toute loi applicable, y compris les lois sur le contrôle des exportations des États-Unis ou les lois sur les brevets, les marques de commerce ou le droit d'auteur des États-Unis.

¹² Voir D.C. Official Code § 38-831.03(a).

¹³ Disponible sur <https://dcps.dc.gov/page/assistive-technology%E2%80%AF>.

¹⁴ Pour plus d'informations sur le dépôt de rapports et de plaintes, veuillez consulter la section V.

4. Constitue une utilisation à des fins obscènes ou pornographiques ou à l'appui de telles fins, y compris, mais sans s'y limiter, la transmission, la récupération ou la visualisation de tout matériel profane, obscène ou sexuellement explicite ;
5. Constitue une utilisation pour solliciter ou distribuer des informations dans le but d'inciter à la violence, de causer un préjudice personnel ou des blessures corporelles, ou de harceler, menacer ou traquer une autre personne ;
6. Contient un virus, un cheval de Troie, un rançongiciel ou tout autre composant nuisible ou code malveillant ;
7. Constitue du courrier indésirable, du hameçonnage, du spam ou de la diffusion non autorisée d'e-mails ;
8. Viole la sécurité de tout autre appareil ou réseau de DCPS, ou constitue un accès non autorisé à tout appareil ou réseau de DCPS ou tente de contourner toute mesure de sécurité ;
9. Obtient l'accès ou fournit à un tiers non autorisé l'accès au compte, aux fichiers ou aux données d'un autre utilisateur sur le réseau de DCPS, ou modifie ses fichiers, données ou mots de passe ;
10. Se fait passer pour toute personne autorisée vivante ou décédée, organisation, entreprise ou autre entité, dans l'intention de tromper ;
11. Dégrade les performances du réseau ou de la technologie de DCPS, entraîne un risque de sécurité pour le réseau ou la technologie de DCPS ou menace de toute autre manière l'intégrité ou le fonctionnement efficace du réseau ou de la technologie de DCPS ;
12. Prive un utilisateur autorisé de l'accès au réseau ou à la technologie de DCPS ;
13. Obtient un accès à la technologie ou au réseau de DC au-delà de ce qui est autorisé ;
14. Entreprend une entrée non autorisée ou illégale dans un système du réseau de DCPS ;
15. Divulgue des informations confidentielles ou exclusives, y compris des informations sur les dossiers d'élèves, sans autorisation ou sans mesures de sécurité appropriées ;
16. Divulgue ou transmet des informations, des vidéos et des photographies personnelles identifiables d'élèves sans autorisation ou sans mesures de sécurité appropriées ;
17. Partage des renseignements confidentiels sur des élèves ou du personnel de DCPS d'une manière qui enfreint la loi de DC, la loi fédérale, les réglementations, les politiques ou les lignes directrices ;
18. Partage des adresses e-mail ou des listes de distribution de DCPS pour des utilisations qui violent la présente politique ou toute autre politique de DCPS ;
19. Permet ou constitue des paris ou des jeux de hasard de quelque nature que ce soit ;
20. Installe, télécharge ou utilise un système tiers ou un logiciel non autorisé ou sans licence ;
21. Accède à, distribue, télécharge ou utilise des jeux, programmes, fichiers, médias électroniques ou applications autonomes non autorisés à partir d'Internet qui peuvent constituer une menace pour le réseau de DCPS ;
22. Fait la promotion de tombolas ou de collectes de fonds non autorisés ou y participe de quelque manière que ce soit ;
23. Fait la promotion d'activités politiques partisans ou y participe de quelque manière que ce soit ;
24. Fait la promotion d'activités politiques ou électorales internes liées à un syndicat ou à une autre organisation représentant les employés ou y participe de quelque manière que ce soit ;
25. Se livre à des activités commerciales privées ou à d'autres activités à des fins de gain financier personnel ;
26. Distribue des informations non autorisées concernant les systèmes de sécurité ou les mots de passe d'autres utilisateurs ;

27. Falsifie, altère les données situées sur le réseau de DCPS ou sur tout système scolaire ou y apporte des modifications, des ajouts ou des suppressions non autorisés ;
28. Accède à ou utilise des données situées sur un réseau de DCPS à des fins personnelles ;
29. Favorise toute activité ou relation avec un élève qui n'est pas liée aux activités scolaires ou extrascolaires parrainées par l'école ou y participe, sauf autorisation écrite préalable du chef d'établissement et du parent/tuteur de l'élève ;
30. Viole les conditions d'utilisation spécifiées d'une technologie, d'une application ou d'un système du réseau de DCPS particulier ;
31. Constitue une utilisation qui perturbe le bon fonctionnement d'une école ou d'un bureau ;
32. Se livre au piratage (c'est-à-dire obtenir intentionnellement un accès par des moyens illégaux ou sans autorisation) du réseau de DCPS pour accéder à des informations non autorisées ou pour contourner les systèmes de sécurité des informations ;
33. Adopte des comportements sexuels inappropriés, y compris un contact sexuel non désiré, une exposition indécente, la transmission d'images à connotation sexuelle ou d'autres activités sexuelles ; ou
34. Enfreint toute interdiction mentionnée dans la présente politique ou dans toute autre politique de DCPS.

Les élèves, le personnel et les autres utilisateurs ne doivent pas partager leur appareil délivré par DCPS ou leurs informations de connexion au réseau fournies par DCPS avec quiconque. Il est strictement interdit d'utiliser l'appareil délivré par DCPS ou les informations de connexion au réseau fournies par DCPS de quelqu'un d'autre, de permettre à des utilisateurs non autorisés d'utiliser son appareil délivré par DCPS ou ses informations de connexion au réseau fournies par DCPS, ou de faciliter l'utilisation non autorisée de l'appareil délivré par DCPS ou des informations de connexion au réseau fournies par DCPS d'une autre personne par le biais du partage d'informations de connexion ou par tout autre moyen.

E. Technologie personnelle

L'utilisation par les élèves d'une technologie personnelle sur le réseau de DCPS n'est pas autorisée sans l'autorisation écrite expresse du chancelier ou de son représentant. DCPS n'est pas responsable de l'entretien et de la sécurité des appareils électroniques personnels des élèves et n'assume aucune responsabilité en cas de perte ou de vol. DCPS, le Bureau du directeur de la technologie de DC et leur personnel ne sont pas tenus de fournir une assistance technique aux élèves qui souhaitent utiliser des appareils électroniques personnels à l'école ou sur le réseau de DCPS, ou accéder à des comptes de médias personnels sur des appareils de DCPS, en dehors de l'assistance relative aux applications Web approuvées par DCPS qui sont utilisées sur ces appareils personnels. Sauf dans les cas décrits ci-dessous dans la présente section, DCPS se réserve le droit d'appliquer des mesures de sécurité sur les appareils personnels lorsqu'ils sont utilisés pour accéder au réseau de DCPS et de supprimer les appareils jugés en violation de la politique de DCPS.

F. Confidentialité de la technologie et des comptes de médias personnels des élèves

1. Politiques relatives à la technologie et aux comptes de médias personnels des élèves spécifiques à l'école

Les chefs d'établissement doivent informer les élèves et les parents par écrit si leur école a des règles supplémentaires concernant les comptes de médias personnels et les appareils technologiques des élèves.

2. Confidentialité générale des appareils technologiques et des comptes de médias personnels des élèves

Hormis les exceptions prévues à la section IV.F.3, DCPS ne prendra ni ne menacera de prendre de mesures à l'encontre d'un élève ou d'un futur élève, y compris des mesures disciplinaires, l'expulsion, la désinscription, le refus d'admission ou l'interdiction de participer à une activité scolaire ou extrascolaire, parce que l'élève ou le futur élève a refusé de :

- Divulguer un nom d'utilisateur, un mot de passe ou tout autre moyen d'authentification de compte utilisé pour accéder à son compte de média personnel ou à son appareil technologique personnel ;
- Accéder à son compte de média personnel ou à son appareil technologique personnel en présence du personnel de l'école de manière à permettre au personnel de l'école d'observer les données figurant sur le compte ou l'appareil ;
- Ajouter une personne à la liste des utilisateurs pouvant consulter son compte de média personnel ou accéder à son appareil technologique personnel ; ou
- Modifier les paramètres de confidentialité associés à son compte de média personnel ou à son

appareil technologique personnel¹⁵.

Si DCPS reçoit par inadvertance le nom d'utilisateur, le mot de passe ou d'autres moyens d'authentification de compte associés au compte de média personnel ou à l'appareil technologique personnel d'un élève ou d'un futur élève par des moyens par ailleurs légaux, DCPS :

- N'utilisera pas ces informations pour accéder au compte de média personnel ou à l'appareil technologique personnel de l'élève ou du futur élève ;
- Ne partagera pas ces informations avec quiconque ; et
- Supprimera ces informations immédiatement ou dès que cela est raisonnablement possible¹⁶.

Rien dans cette section n'empêche DCPS de :

- Accéder aux informations sur un élève ou un futur élève qui sont accessibles au public ;
- Demander à un élève ou à un futur élève de partager volontairement un contenu précis accessible à partir d'un compte de média personnel ou d'un appareil technologique personnel dans le but de garantir le respect des lois applicables ou des politiques de DCPS, à condition que la demande soit conforme aux exigences de la présente politique ;
- Interdire à un élève ou à un futur élève d'accéder à ou d'utiliser un compte de média personnel ou un appareil technologique personnel pendant les heures de classe ou dans l'enceinte de l'école ;
- Surveiller l'utilisation du réseau de DCPS ; ou
- Révoquer l'accès d'un élève, en tout ou partie, au réseau ou à la technologie de DCPS¹⁷.

3. Exceptions à la confidentialité de la technologie et des comptes de médias personnels des élèves

Le personnel de DCPS peut effectuer des recherches sur le compte de média personnel ou l'appareil technologique personnel d'un élève ou obliger un élève à produire des données accessibles à partir de son compte de média personnel ou de son appareil technologique personnel dans les cas suivants de violation de la politique ou de menace imminente pour la vie ou la sécurité.

a. Violation de la politique

Le personnel de DCPS peut effectuer des recherches sur le compte de média personnel ou l'appareil technologique personnel d'un élève ou obliger un élève à produire des données accessibles à partir de son compte de média personnel ou son appareil technologique personnel si le personnel de DCPS a des motifs raisonnables de soupçonner que l'élève a utilisé ou utilise son compte de média personnel ou son appareil technologique personnel pour commettre une violation de la politique de DCPS et a des motifs raisonnables de soupçonner que le compte de média personnel ou l'appareil technologique personnel de l'élève contient des preuves de la violation présumée¹⁸.

¹⁵ D.C. Official Code § 38-831.04(a).

¹⁶ D.C. Official Code § 38-831.04(b).

¹⁷ D.C. Official Code § 38-831.04(e).

¹⁸ D.C. Official Code § 38-831.04(c)(1)(A).

Avant de procéder à une telle recherche ou d'obliger l'élève à produire de telles données, le personnel de DCPS doit :

- Documenter les soupçons raisonnables justifiant la nécessité de la recherche ou de la production ; et
- Informer l'élève et le parent/tuteur de l'élève de la violation présumée et des données ou composants qui seront recherchés ou que l'élève sera obligé de produire¹⁹.

DCPS peut saisir l'appareil technologique personnel d'un élève pour empêcher la suppression des données en attendant cette notification requise, uniquement si la période de saisie préalable à la notification ne dépasse pas 48 heures et que l'appareil technologique personnel est stocké en toute sécurité sur la propriété de DCPS et n'est pas consulté pendant la période de saisie préalable à la notification²⁰.

La recherche ou la production forcée doit être limitée aux données accessibles à partir du compte ou de l'appareil ou des composants de l'appareil raisonnablement susceptibles de fournir des preuves de la violation présumée, et personne ne peut être autorisé à copier, partager ou transférer des données obtenues à la suite d'une recherche ou d'une production forcée qui ne sont pas liées à la violation présumée qui a motivé la recherche²¹.

b. Menace imminente pour la vie ou la sécurité

Le personnel de DCPS peut effectuer des recherches sur le compte de média personnel ou l'appareil technologique personnel d'un élève ou obliger un élève à produire des données accessibles à partir de son compte de média personnel ou de son appareil technologique personnel, si cela est nécessaire pour répondre à une menace imminente pour la vie ou la sécurité²².

La portée de toute recherche ou production forcée doit être limitée à cette fin et DCPS doit, dans les 72 heures suivant la recherche ou la production forcée, fournir à l'élève et à son parent une description écrite de la menace précise qui a motivé la recherche et des données qui ont été consultées²³.

V. EXIGENCES DE MISE EN ŒUVRE DE LA POLITIQUE

Tous les élèves et membres du personnel de DCPS sont tenus de se conformer aux exigences énoncées dans la présente politique. Pour soutenir sa mise en œuvre, les chefs d'établissement doivent informer chaque année le personnel des activités et des délais requis. La mise en œuvre de la présente politique sera renforcée par un processus de surveillance central, qui comprend des examens réguliers des données, un échantillonnage des dossiers, des examens de la documentation sous-jacente et des visites sur place (au besoin). Ce cadre nous permettra de collaborer pour construire un système d'amélioration continue et prévenir la non-conformité. Pour obtenir des orientations clés et une assistance en matière de questions, de formation ou de mise en œuvre, veuillez consulter dcps.dc.gov.

¹⁹ D.C. Official Code § 38-831.04(c)(1)(B).

²⁰ D.C. Official Code § 38-831.04(d).

²¹ D.C. Official Code § 38-831.04(c)(1)(C)-(D).

²² D.C. Official Code § 38-831.04(c)(2)(A).

²³ D.C. Official Code § 38-831.04(c)(2)(B)-(C).

DCPS s'engage à servir chaque élève avec équité, excellence, transparence et responsabilité. Pour toute préoccupation concernant cette directive ou pour signaler des violations potentielles de celle-ci, contactez le directeur de l'intégrité en remplissant le formulaire de référence en ligne²⁴ ou en envoyant un e-mail à dcps.cio@k12.dc.gov.

²⁴ Disponible sur <https://dcps.dc.gov/page/office-integrity>.

ANNEXES

Les documents suivants sont inclus en annexe :

- Accord d'utilisation responsable de la technologie par l'élève ;
- Formulaire d'accusé de réception de l'Accord d'utilisation responsable de la technologie par l'élève ; et
- Formulaire d'accusé de réception de l'Accord d'utilisation responsable de la technologie par le personnel.



Accord d'utilisation responsable de la technologie par l'élève

En tant qu'utilisateur responsable de la technologie :

A. Je traiterai mon appareil de DCPS avec respect, en prenant soin de ne pas le laisser tomber ou l'endommager.

- Je suivrai les règles de l'école concernant l'emprunt et le retour de mon appareil de DCPS.
- Si mon appareil de DCPS est endommagé ou ne fonctionne pas correctement, je le signalerai immédiatement à un enseignant ou à un membre du personnel.
- Je garderai mon appareil à l'intérieur en lieu sûr quand je ne l'utiliserai pas.

B. Je protégerai mes renseignements personnels.

- Je ne partagerai mon appareil de DCPS, mon nom d'utilisateur ou mon mot de passe avec personne (sauf si je suis un élève de la petite enfance ou un élève qui a besoin d'aide pour utiliser son compte).
- Je sauvegarderai mon travail dans mon Office 365 OneDrive de DCPS et me déconnecterai de mes comptes et programmes lorsque j'aurai fini de travailler.
- J'informerai immédiatement un enseignant si je pense ou si je sais que quelqu'un a utilisé mon compte.

C. J'utiliserai mon appareil uniquement pour mes devoirs scolaires.

- Je ne téléchargerai, installerai ou utiliserai des logiciels, des applications, des extensions de navigateur ou des fichiers multimédias que si mon professeur m'y autorise.
- J'éviterai les ressources inappropriées, offensantes ou illégales. Si je vois du matériel inapproprié en ligne, je le signalerai immédiatement à un enseignant ou à un membre du personnel.

D. J'utiliserai mes compétences en matière de [citoyenneté numérique](#) et traiterai les gens avec gentillesse.

- J'utiliserai un langage respectueux et approprié.
- Je ferai correctement référence au travail des autres et je ne ferai pas de plagiat.
- Je vérifierai les informations avant de les partager en ligne.
- J'utiliserai l'IA de manière responsable et éthique, en respectant la vie privée de tous, en ne harcelant ni n'intimidant personne, et en ne plagiant ni ne trichant dans mes devoirs scolaires.

Résultats d'une utilisation irresponsable de la technologie

Vous perdrez l'accès au réseau ou à la technologie de DCPS pendant des périodes croissantes en vertu de la réglementation et des politiques disciplinaires visant les élèves de DCPS. Dans certaines circonstances, le personnel de DCPS peut être autorisé à rechercher et à consulter à tout moment tous les fichiers situés sur le réseau de DCPS ou enregistrés sur les appareils de DCPS. Dans certaines circonstances, le personnel de DCPS peut être autorisé à faire des recherches dans votre compte de média personnel ou votre appareil ou vous demander de produire des données à partir de votre compte de média personnel ou de votre appareil.

Protocole pour les appareils volés ou endommagés accidentellement

Si votre appareil a été volé ou endommagé, vous devez immédiatement en informer un enseignant ou un membre du personnel dès que possible, car DCPS doit déposer un rapport de police dans les cinq



jours civils suivant un vol présumé afin que l'appareil puisse être localisé. Vous ne serez pas tenu responsable des frais associés à l'appareil volé ou accidentellement endommagé. Votre collaboration avec DCPS est grandement appréciée dans ce scénario.

Exemples d'utilisation inacceptable de la technologie :

- Manger ou boire à proximité d'un appareil de DCPS ;
- Écrire, dessiner ou coller des autocollants sur un appareil de DCPS ;
- Télécharger, installer ou exécuter tout type de fichiers, y compris des fichiers musicaux et vidéo, des sites Web, des logiciels, des applications, des extensions de navigateur ou des médias, sauf si un enseignant l'autorise ;
- Utiliser des applications ou des modules d'extension pour tenter de modifier les paramètres de sécurité ou les filtres de contenu Internet ;
- Insérer des clés USB dans un appareil, sauf si un enseignant l'autorise ;
- Rechercher, sauvegarder, diffuser ou afficher des ressources haineuses, obscènes, vulgaires, etc. ;
- Utiliser le réseau de DCPS pour se livrer à des actes illégaux ou criminels ;
- Accéder à des jeux en ligne, à des réseaux sociaux, à des applications de messagerie ou à des discussions de groupe, sauf si ces activités sont liées aux devoirs scolaires et qu'un enseignant ou un membre du personnel supervise l'activité ;
- Intimider, harceler ou menacer d'autres personnes ;
- Utiliser le nom de connexion ou le mot de passe d'une autre personne ; et
- Créer ou publier des photos ou des enregistrements audio ou vidéo d'autres personnes sans leur autorisation.



Formulaire d'accusé de réception de l'Accord d'utilisation responsable de la technologie par l'élève

Élèves : J'ai lu la Politique d'utilisation acceptable de la technologie et du réseau par les élèves et le personnel de DCPS et l'Accord d'utilisation responsable de la technologie par l'élève, ou quelqu'un me les a lus et expliqués.

Parents/tuteurs : J'ai lu la Politique d'utilisation acceptable de la technologie et du réseau par les élèves et le personnel de DCPS et l'Accord d'utilisation responsable de la technologie par l'élève et j'en ai discuté avec mon enfant.

1. J'accepte d'utiliser tous les appareils de DCPS et le réseau de DCPS de manière responsable, conformément aux règles énumérées dans l'Accord et la Politique d'utilisation acceptable. Je comprends que si je ne respecte pas ces règles, je peux subir des conséquences en vertu des règles et politiques disciplinaires de DCPS et ma capacité à utiliser les appareils de DCPS et le réseau de DCPS peut être restreinte.
2. Je comprends que si je vois ou deviens autrement conscient que quelqu'un utilise un appareil de DCPS ou le réseau de DCPS pour intimider, menacer, harceler ou nuire à quelqu'un d'autre, je devrai le signaler à un enseignant ou à un membre du personnel. Je comprends que mon signalement restera confidentiel et que DCPS ne tolérera aucune représailles à mon encontre pour avoir fait un signalement.
3. Si je reçois un appareil, je comprends qu'il est prêté uniquement à moi et conformément à la Politique d'utilisation acceptable de la technologie et du réseau par les élèves et le personnel de DCPS. DCPS collecte des données et surveille l'utilisation de l'ordinateur portable conformément à la Protecting Students Digital Privacy Act de 2016.
4. Si je perds ou endommage intentionnellement ou par négligence un appareil de DCPS, je pourrais faire face à des mesures disciplinaires appropriées de la part de DCPS. Je devrai rencontrer DCPS pour déterminer la raison de la perte ou du dommage et apprendre les pratiques responsables d'entretien des appareils.
5. Si je reçois un appareil, je comprends qu'il doit être retourné sur demande au point de contact de la technologie de mon école ou à l'équipe informatique de DCPS (AssetAdmin@k12.dc.gov). Si je ne retourne pas l'appareil comme demandé, l'appareil pourrait être désactivé à distance et des frais pourraient être facturés à ma famille.
6. Je comprends que je n'aurai plus accès à la technologie ou au réseau de DCPS une fois que j'aurai obtenu mon diplôme ou que je quitterai DCPS.



Formulaire d'accusé de réception de l'Accord d'utilisation responsable de la technologie par le personnel

J'ai lu la Politique d'utilisation acceptable de la technologie et du réseau par les élèves et le personnel.

1. J'accepte d'utiliser le réseau de DCPS et tout appareil de DCPS qui m'a été fourni de manière responsable, conformément aux règles énumérées dans la Politique d'utilisation acceptable. Je comprends que si je ne respecte pas ces règles, je pourrais subir des conséquences en vertu des règles et politiques disciplinaires de DCPS ainsi que des lois et réglementations de DC.
2. Si DCPS me fournit un ordinateur portable, je reconnais que cet ordinateur portable appartient à DCPS. L'ordinateur portable m'est prêté pour être utilisé uniquement à des fins professionnelles et conformément à la Politique d'utilisation acceptable de la technologie et du réseau par les élèves et le personnel de DCPS.
3. Si DCPS me fournit un ordinateur portable, je suis responsable de tous les coûts associés à la réparation des dommages causés par ma négligence ou mes actions intentionnelles pendant le prêt de l'ordinateur portable.
4. Si DCPS me fournit un ordinateur portable, celui-ci doit être retourné à l'équipe informatique de DCPS (AssetAdmin@k12.dc.gov) si je quitte l'organisation ou sur demande. Le fait de ne pas retourner cet appareil à la demande de DCPS peut entraîner la facturation de frais à mon égard.