RÈGLEMENT

MONTGOMERY COUNTY PUBLIC SCHOOLS

'Sources connexes : BBB, EDC, EDC-RA, EGI-RA, EHC-RA, IGS, JFA, JFA-RA, JHF-RA, JOA-RA, KBA-RB**,** KBB
Bureau responsable : Surintendant des écoles

Responsabilités de l'utilisateur de systèmes informatiques, d'informations électroniques et sécurité des réseaux

I. OBJECTIF

A. Assurer la sécurité de tous les éléments constitutifs des systèmes informatiques de Montgomery County Public Schools (MCPS), de la technologie liée et des informations électroniques ;

B. Définir les limites d'un usage dit "convenable" pour l'ensemble des utilisateurs de systèmes informatiques de MCPS ;

C. Promouvoir le développement intellectuel grâce à l'utilisation de systèmes informatiques, de technologies connexes et d'informations électroniques dans un environnement sûr ; et

D. Assurer la conformité aux lois nationales, locales et fédérales en vigueur.

II. CONTEXTE

MCPS met à disposition du matériel informatique, des services informatiques, et l'accès au réseau des écoles et des bureaux administratifs en vue d'atteindre des objectifs en harmonie avec la mission de MCPS. La grande diversité de technologie de l'information disponible aux élèves de MCPS est synonyme de nouveaux risques ainsi que de nouvelles opportunités. La responsabilité d'un comportement convenable incombe à toutes les personnes qui utilisent les ressources informatiques et les installations informatiques de MCPS. Dans les écoles, les activités en ligne des élèves mineurs sont surveillées par le personnel grâce à des mesures de protection technologiques à l'échelle du groupe scolaire. Les niveaux d'accès sont fournis en fonction de l'affectation, la responsabilité et du besoin de savoir. Les utilisateurs doivent protéger les informations et les ressources contre le vol, la dégradation intentionnelle, l'accès non autorisé, la falsification et la perte.

III. DÉFINITIONS

A. Une *méthode de signature électronique approuvée* se définie par une méthode approuvée au préalable par le Surintendant des écoles et/ou son délégué, en application du présent règlement et à toutes les lois nationales et fédérales en vigueur, et qui précise la forme que revêt la signature électronique, les systèmes et procédures utilisés avec la signature électronique et l'importance de l'utilisation de celle-ci.

B. Un *système informatique* se réfère a du matériel, des logiciels et des technologies connexes, notamment les réseaux, le câblage et les équipements de communication.

C. *La cyberintimidation et/ou le harcèlement ou la menace par voie électronique* se définit par une conduite intentionnelle utilisant des communications électroniques telles que le courrier électronique (e-mail), la messagerie instantanée, les sites de réseaux sociaux, le blog, les téléphones portables ou d'autres moyens technologiques pour créer de un environnement éducatif hostile en perturbant de manière significative les bienfaits, les opportunités ou la performance éducative d'un élève, ou en perturbant son bien-être physique ou psychologique, et qui est :

- motivé par une caractéristique personnelle réelle ou perçue, notamment la race, l'origine nationale, l'état matrimonial, le sexe, l'orientation sexuelle, l'identité de genre, la religion, l'ascendance, les attributs physiques, le statut socio-économique, le statut familial, ou l'aptitude physique ou mentale ou le handicap ; ou,

- est menaçant ou sérieusement intimidant ; et,

- a lieu sur la propriété scolaire, durant une activité ou un évènement scolaire, ou dans un autobus scolaire ; ou

- perturbe de manière considérable le bon fonctionnement de l'école

D. *Les objectifs pédagogiques* sont les actions qui promeuvent directement les missions éducatives, pédagogiques, administratives, commerciales et de soutien de MCPS et qui sont liées à tout enseignement, projet, emploi, travail affecté, tâche ou fonction, dont l'utilisateur est responsable.

E. *Les données et informations électroniques* sont des faits ou des chiffres sous toute forme électronique ou numérique, tels que par exemple : le courrier électronique, la messagerie instantanée, les salles de chat (chat rooms), les SMS, les documents, les bases de données, les fichiers, les sites Internet et toute autre information stockée électroniquement.

F. Un *dossier électronique* est une information générée, envoyée, reçue ou stockée sous forme numérique dans le cadre de la conduite des activités de MCPS, communiquée entre les parties comme preuve d'une transaction et conservée dans le cadre de l'archivage de MCPS. Un dossier ne contient pas d'informations dont le caractère transitoire fait qu'elles ne sont généralement pas conservées.

G. Une *signature électronique* est un son, un symbole ou un processus électronique, attaché ou associé logiquement à un dossier électronique et exécuté ou adopté par une personne avec l'intention de signer un contenu.

H. *Le contenu inapproprié* désigne un contenu obscène ou pornographique et donc nocif pour les mineurs/élèves, notamment les sites Internet en lien avec du contenu adulte ou à caractère sexuel, le contenu inadapté à l'âge et le contenu qui n'a aucune vocation éducative, tel que défini dans le présent règlement, ou le contenu incompatible avec la sécurité du système ou les politiques et les règlements de MCPS. Le contenu inapproprié peut également inclure ce qui incite ou promeut le piratage, l'utilisation, la distribution et la production de drogues, d'alcool et de tabac, l'intimidation, le harcèlement et les menaces, l'acquisition de compétences criminelles, la violence ou l'utilisation ou la possession illégale d'armes. Lorsque la nécessité d'une recherche de bonne foi ou à d'autres fins licites est identifiée par le personnel, un accès adapté peut être accordé.

I.L' *accès Internet* comprend toutes les méthodes autorisées utilisées pour se connecter aux serveurs et aux utilisateurs Internet, ainsi que toutes les méthodes autorisées pour fournir l'accès.

J. Une *mesure de protection de la technologie* est une technologie de filtrage Internet conçue pour limiter l'accès à certaines zones d'Internet en fonction de critères précis conçus pour limiter ou empêcher l'accès à du contenu inapproprié.

K. Un *équipement non autorisé* se définit par tout appareil qui n'a pas reçu l'approbation du Bureau du Responsable de la technologie (OCTO) et/ou son représentant pour être connecté à un ordinateur ou un réseau de MCPS, tel que notamment les ordinateurs, les tablettes, les appareils de communication et d'organisation personnels tels que points d'accès sans fil, smartphones ou téléphones portables ; les appareils de jeu vidéo ; les équipements photographiques ; et les appareils de divertissement tels que lecteurs MP3 ou les iPods™.

L. Un *utilisateur* est tout membre du personnel MCPS, élève ou toute autre personne autorisée à utiliser les systèmes informatiques MCPS. Les autres personnes peuvent inclure les parents, les bénévoles et le personnel contractuel ou temporaire.

IV. PROCÉDURES

Le paragraphe suivant définit les procédures requises pour la cybersécurité, la cybersûreté et la cyberéthique pour la sécurité des données et des informations électroniques, les transactions et signatures électroniques, la sécurité physique, la sécurité des systèmes et des applications, ainsi que la sécurité, l'utilisation et la conduite des réseaux. Des directives de responsabilité de l'utilisateur et procédures plus spécifiques pour la sécurité des systèmes informatiques sont développées dans le *Manuel des procédures de sécurité des systèmes informatiques de MCPS* disponible sur le site Internet de MCPS.

A. Sécurité des données et des informations électroniques

Les utilisateurs ne peuvent accéder qu'aux informations et/ou aux systèmes informatiques auxquels ils sont autorisés et dont ils ont besoin dans le cadre de leur mission et leurs responsabilités.

1. Les utilisateurs sont responsables de leurs propres comptes individuels.

    a) Les utilisateurs doivent changer leurs mots de passe au besoin et garder leurs mots de passe strictement confidentiels.

    b) Il est expressément interdit aux utilisateurs de partager leur compte et communiquer leurs mots de passe.

    c) Toute violation pouvant être attribuée à un nom de compte individuel sera traitée comme la responsabilité du propriétaire du compte.

2. Les utilisateurs doivent se déconnecter de tous les systèmes avant de quitter un ordinateur ou un poste de travail ou d'autoriser d'autres personnes à l'utiliser.

3. Il incombe à chaque utilisateur de connaître et suivre les procédures de sécurité conformément à ce règlement.

4. Les utilisateurs sont tenus de sécuriser leurs données électroniques. (Remarque : les fichiers sensibles doivent être enregistrés dans un emplacement sécurisé tel que le dossier/répertoire réseau d'un individu ou un disque dur externe destiné à être ensuite sécurisé dans une armoire à fichiers verrouillée.)

5. MCPS n'est pas responsable des informations susceptibles d'être perdues en raison de panne ou d'interruption du système. Les utilisateurs doivent faire des copies de sauvegarde et s'assurer que celles-ci sont stockées dans un endroit sûr.

B. Transactions et signatures électroniques

Lorsque la loi de l'État du Maryland, la loi fédérale ou les politiques ou réglementations de MCPS exigent qu'une transaction porte la signature d'une personne autorisée, cette exigence est satisfaite lorsque le fichier électronique peut recevoir une signature électronique qui fonctionne sur la base d'une méthode de signature électronique approuvée. Les procédures d'autorisation et d'utilisation des transactions et signatures électroniques sont décrites dans le *Manuel des procédures de sécurité des systèmes informatiques de MCPS*.

C. Sécurité physique

Les équipements des systèmes informatiques doivent être situés et conservés dans un environnement physique sécurisé. Les utilisateurs sont responsables du respect des dispositions de sécurité physique pour les ordinateurs et les technologies liées.

1. Lorsque les membres du personnel ne sont pas présents pour superviser la zone, toutes les zones (y compris le stockage permanent ou temporaire) abritant du matériel informatique précieux doivent être sécurisées.

2. Les ordinateurs ou leurs équipements connexes ne peuvent pas être retirés de la propriété de MCPS sans autorisation appropriée.

3. Les utilisateurs doivent utiliser des procédures de responsabilité locales pour se connecter ou se déconnecter de tout ordinateur ou équipement connexe. Ces équipements doivent être restitués à l'école, au département, à la division ou à l'unité qui les possède avant que l'utilisateur ne quitte MCPS ou soit transféré vers une autre école ou un autre bureau.

4. Le stock local d'équipements sera maintenu avec autant de précision que possible. Les équipements seront ajoutés aux stocks après leur acquisition. Les utilisateurs ne doivent pas retirer des ordinateurs les repères ou les étiquettes liés au stockage.

5. Le matériel perdu et volé doit être traité conformément au règlement EDC-RA de MCPS, *Contrôle des stocks de mobilier et d'équipements*.

D. Sécurité des systèmes et des applications

1. Les utilisateurs ne doivent pas installer de logiciels ou de matériel, ni désactiver ou modifier les paramètres ou mesures de sécurité (tels que les logiciels antivirus) installés sur un ordinateur ou d'autres appareils numériques/électroniques autorisés à quelque fin que ce soit sans autorisation du personnel approprié, selon les termes du *Manuel des procédures de sécurité des systèmes informatiques de MCPS*.

2. Les utilisateurs ne doivent pas modifier les paramètres système sans autorisation du personnel en charge, en application du *Manuel des procédures de sécurité des systèmes informatiques de MCPS*.

3. Les logiciels et applications de MCPS ne peuvent pas être installés ou copiés sur un ordinateur non MCPS, sauf indication contraire dans les accords de licence.

E. Sécurité des réseaux

Tout accès au réseau et aux informations de MCPS nécessite l'approbation d'une autorité de MCPS agréée par l'OCTO. Les comptes d'utilisateurs ou l'accès peuvent être supprimés, suspendus ou révoqués s'il est établi que l'accès au réseau ou à l'information est utilisé en violation de cette politique ou de toute autre politique ou réglementation en vigueur de MCPS.

F. Conduite et utilisation

L'utilisation d'Internet par les élèves et le personnel sera surveillée par diverses méthodes, notamment la technologie et la supervision directe.

1. Il incombe aux utilisateurs de s'assurer que l'accès ou l'importation de matériel sur les réseaux ait une vocation éducative telle que définie dans le présent règlement.

2. Tout matériel ou information volontairement publié ou lié à partir d'un système de MCPS ou d'un site Internet doit être conforme à l'objectif pédagogique, tel que défini dans le présent règlement.

3. Les utilisateurs sont responsables du respect des règles applicables au(x) système(s) informatique(s) qu'ils utilisent, y compris ceux accessibles via Internet à partir des équipements de MCPS.

4. MCPS n'a aucun contrôle et ne peut être tenu responsable des informations résidant sur d'autres systèmes ou sites Internet disposant d'un accès via

MCPS. Certains sites et systèmes extérieurs à MCPS peuvent contenir du matériel diffamatoire, inexact, abusif, obscène, profane, à caractère sexuel, menaçant, racialement offensant ou illégal.

5. Toute utilisation des installations informatiques, des réseaux et d'autres ressources technologiques doit avoir une vocation éducative, selon les termes du paragraphe III.D., et est soumise à l'examen de MCPS, et peut être enregistrée et archivée.

6. L'e-mail de MCPS est uniquement destiné à un usage à vocation éducative. Toutes les actions sont soumises à la révision de MCPS et peuvent être notées et archivées. Toute utilisation par les élèves de l'e-mail de MCPS doit être autorisée à des fins de soutien ou de mise en place du processus d'apprentissage.

7. Il est interdit aux élèves d'utiliser un e-mail, une messagerie instantanée ou un forum de discussion non-autorisé.

8. Bien qu'il soit impossible de documenter toute conduite et utilisation inappropriées des installations informatiques, les directives suivantes fournissent des exemples d'infractions interdites dans l'utilisation des ordinateurs et des réseaux :

   a) L'altération du système (également connue sous le nom de piratage) ou l'assistance à autrui pour provoquer une altération en fournissant des instructions ou des informations sur la façon d'altérer tout système de MCPS (toute modification non autorisée des systèmes d'exploitation, des comptes individuels, du dossier partagé en réseau, du logiciel, des infrastructures de réseau et/ou autres programmes), et/ou des dommages matériels.

   b) Déchiffrer les mots de passe, les clés de connexion ou la capture non autorisée de mots de passe à l'aide de périphériques matériels ou d'applications logicielles et/ou obtenir un accès ou des privilèges de niveau supérieur non autorisé ou tenter de le faire.

   c) Interférer délibérément avec l’accès au réseau des autres utilisateurs ou l’utilisation de l’ordinateur, par exemple par déni de service (DoS) ou déni de service distribué (DDoS).

   d) Faire des déclarations ou des actions calomnieuses, diffamatoires ou constituant de la cyberintimidation, du harcèlement ou de la menace d'autrui.

e) Accéder en connaissance de cause ou tenter d'accéder à du matériel inapproprié, comme indiqué en III. H. Ci-dessus.

f) Présenter des codes/logiciels malveillants tels que des virus ou malwares capables de causer des dommages ou d'altérer la fonction prévue des systèmes informatiques de MCPS.

g) Attacher un équipement non autorisé à tout ordinateur ou au réseau de MCPS sans l'autorisation d'OCTO et/ou de son représentant.

h) Utiliser le courrier électronique pour harceler ou escroquer d'autres personnes en envoyant des messages en masse et/ ou commerciaux menaçants ou non sollicités sur Internet, ou en utilisant des messages électroniques frauduleux pour obtenir des informations personnelles à des fins de vol d'identité.

i) Confiner les mesures technologiques de protection, également appelées technologies de sécurité ou de filtrage du réseau, par l'utilisation de serveurs proxy, d'applications ou d'autres méthodes.

j) Supprimer, falsifier, modifier ou lire ou copier sans autorisation le courrier électronique (e-mail) d'autres utilisateurs ou tenter de le faire.

k) Lire, supprimer, copier, transmettre, imprimer, partager ou modifier les fichiers de données d'autres utilisateurs sans l'autorisation du directeur des écoles et/ou de son représentant.

l) Autoriser une personne tierce à utiliser son adresse e-mail, son compte ou son mot de passe MCPS personnel.

m) Autoriser une personne tierce à utiliser son compte réseau MCPS personnel, ses dossiers réseau ou son mot de passe.

n) Utiliser des publicités commerciales, des chaînes de lettres ou des jeux non éducatifs sur les systèmes de MCPS.

o) Copier ou transférer du matériel et des logiciels protégés par des droits d'auteur sans autorisation.

p) Publier sur Internet ou diffuser par des moyens électroniques des informations personnellement identifiables sans autorisation ou

publier de fausses informations sur les élèves ou le personnel, en utilisant les équipements ou les ressources de MCPS.

q) Utiliser les réseaux ou systèmes informatiques de MCPS à des fins personnelles ou pour toute activité illégale.

9. Il est interdit à tous les utilisateurs de participer sciemment à la divulgation, l'utilisation et la diffusion non autorisées d'informations personnelles sur des mineurs.

10. Les élèves doivent recevoir une éducation quant au comportement en ligne convenable à adopter, notamment au sujet des d'interactions avec d'autres personnes sur les sites de réseau social et dans les salles de discussion (chat rooms), et sur la sensibilisation et la réaction à avoir face à la cyberintimidation.

11. Tout utilisateur de systèmes informatiques de MCPS qui identifie une zone d'Internet contenant des éléments inappropriés et qui n'ont pas été filtrés par le biais de la mesure de protection technologique, doit spontanément et conformément à la règlementation de suivre les procédures décrites dans le *Manuel de procédures de sécurité des systèmes informatiques de MCPS*, disponibles sur le site Internet de MCPS.

V. NON-CONFORMITÉ

A. Le non-respect des procédures et des normes énoncées dans ce règlement est une cause appropriée de sanctions disciplinaires.

1. Les mesures disciplinaires à l'encontre des employés peuvent se traduire par la participation à une conférence, un avertissement, une lettre de réprimande, une perte de privilèges, une suspension sans salaire, une rétrogradation, un licenciement et/ou des poursuites pénales.

2. Les mesures disciplinaires pour les élèves peuvent inclure notamment et de manière non-exhaustive, un appel téléphonique aux parents ou tuteurs ; une perte de privilèges, la restitution, la suspension et/ou l'expulsion ; et/ou des poursuites pénales. (Voir le règlement JFA-RA de MCPS, *Droits et responsabilités des élèves,* et les politiques de discipline scolaire.)

3. Les actions disciplinaires pour d'autres utilisateurs peuvent inclure la perte de privilèges et/ou des poursuites pénales.

B. Tout utilisateur de systèmes informatiques de MCPS doit signaler une utilisation suspecte ou inappropriée des données, un abus du système informatique ou d'éventuelles violations de la sécurité. Les utilisateurs en milieu scolaire doivent alerter le directeur ou son représentant responsable des technologies de l'information. Les utilisateurs extérieurs au personnel de l'école doivent alerter leurs superviseurs immédiats et le directeur des écoles et/ou son délégué. Les infractions graves, comme indiqué dans le *Manuel des procédures de sécurité des systèmes informatiques de MCPS*, doivent également être signalées à OCTO.

Historique de la règlementation : Nouveau règlement, 22 août 1995 ; révision le 13 décembre 1999 ; intitulés de fonction mis à jour le 1er juin 2000 ; révision le 10 juin 2002 ; révision le 23 mai 2007 ; révision le 27 juillet 2012.