CHARTE INFORMATIQUE

OUTILS INFORMATIQUES NOMADES MISE A DISPOSITION DES EPLE

DIRECTION DE L'EDUCATION ET DE L'ENSEIGNEMENT SUPERIEUR
SERVICE PLANIFICATION | CITE ADMINISTRATIVE TERRITORIALE – CARREFOUR SUZINI 4179 ROUTE DE MONTABO – 97304 CAYENNE – 0594 25 26 37

Table des matières

CHAMP D'APPLICATION 2
INTRODUCTION 2
RÈGLES GÉNÉRALES 3
EQUIPEMENTS DE PRÊT AUX ELEVES 3
Demandes adressées au service planification, déménagement ou une assistance. 3
Configuration du poste de travail 3
RÈGLES GÉNÉRALES DE SÉCURITÉ ET DÉONTOLOGIE 5
Authentification sur les postes de travail 5
Règles de bonnes pratiques 5
Contrôle parental 6
Usages personnels et scolaires 6
Messagerie électronique 7
Internet 7
Téléchargements 8
Réseaux sociaux et comptes personnels 8
Le 3018, un numéro gratuit et une application, pour les victimes de cyberharcèlement 9
Visiteurs, intervenants et prestataires extérieurs 10
RÈGLES D'UTILISATION DES ÉQUIPEMENTS NOMADES - TRAVAIL À LA MAISON 10
Equipements Nomades 10
PROCÉDURES EN CAS DE MOBILITÉ OU DE DÉPART 11
Procédure de départ 11
SÉCURITÉ DU SYSTÈME D'INFORMATION - PANNE & SAV 11
Modalités d'intervention pour les pannes et le service après-vente 11
Accès au poste de travail 12
PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL 12
RESPONSABILITÉS ET SANCTIONS 13
ENTRÉE EN VIGUEUR DE LA CHARTE 14
ANNEXES 15
DISPOSITIONS LÉGALES APPLICABLES 15
RÉFÉRENCES / COORDONNÉES 17
SIGNATURE ET ENGAGEMENT 18

CHAMP D'APPLICATION

La présente charte s'applique à tout utilisateur d'un système d'information mis à disposition par la Collectivité Territoriale de Guyane (CTG) pour l'exercice de ses activités.

On désignera par le terme « utilisateur » toute personne autorisée à accéder aux outils informatiques, système d'information et aux moyens de communication et à les utiliser : élèves, membre de l'administration des Établissements Publics Locaux d'Enseignement (EPLE), agents titulaires ou contractuels, stagiaires, intérimaires, personnes de sociétés prestataires, visiteurs occasionnels, personnels du rectorat, etc.

Le terme « outils informatiques » englobe tous les équipements informatiques, systèmes d'informations et de télécommunications de la collectivité.

INTRODUCTION

La Collectivité Territoriale de Guyane met en œuvre un système d'information et de communication nécessaire à l'exercice de ses activités. Elle met ainsi à disposition des élèves des outils informatiques et de communication.

La présente charte informatique définit les conditions d'accès et les règles d'utilisation des moyens et des ressources informatiques via les outils de communication de la collectivité. Elle a notamment pour but de préciser les droits et les devoirs des utilisateurs.

Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite aux utilisateurs. L'imprudence, la négligence ou la malveillance d'un utilisateur peut avoir des conséquences graves de nature à engager sa responsabilité administrative (CNIL [Commission Nationale de l'Informatique et des Libertés]), civile et/ou pénale et celle de la collectivité.

Le manquement à la présente charte pourra entraîner le retrait du droit d'utilisation d'un outil, d'une application ou d'un matériel informatique/téléphonique et/ou des mesures d'ordre disciplinaire et/ou des sanctions civiles et/ou pénales.

La présente charte s'applique aux élèves, à l'ensemble du personnel tous statuts confondus, y compris au personnel temporaire et occasionnel. Elle s'applique également à tout prestataire extérieur ayant accès aux données et aux outils informatiques de la collectivité ; et à ce titre tout contrat avec un prestataire extérieur devra y faire référence et comporter si besoin la présente charte en annexe.

Dès l'entrée en vigueur de la charte, chaque élève devra en prendre connaissance et devra s'engager à la respecter.

Saisissez-vous de l'opportunité que représente cette charte pour faire de la sécurité un enjeu partagé par l'ensemble des utilisateurs. La sécurité du numérique est assurément l'affaire de tous.

RÈGLES GÉNÉRALES

Les utilisateurs sont supposés adopter un comportement responsable s'interdisant par exemple toute tentative d'accès à des données ou à des sites qui leur seraient interdits.

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes (dégradation, voire interruption de services) sur le fonctionnement du réseau ou des systèmes informatiques ou de télécommunication. Il doit avoir un comportement éthique et en permanence garder à l'esprit que c'est sous le nom de la collectivité qu'il se présente sur Internet et doit se porter garant de l'image de l'institution.

Au même titre que pour le courrier papier ou le téléphone, chacun est responsable des messages envoyés ou reçus, et doit utiliser la messagerie dans le respect de la hiérarchie et des règles élémentaires de courtoisie et de bienséance.

L'utilisation des systèmes d'information doit se faire en conformité avec les procédures et modes d'emploi édictés par les éditeurs et dans le respect des règles de sécurité déployées et de bonnes pratiques recommandées par la Direction des Systèmes d'Information (DSI), la DPD, le législateur et les régulateurs.

EQUIPEMENTS DE PRÊT AUX ELEVES

Demandes adressées au service planification, déménagement ou une assistance.

De manière générale, les demandes sont à adresser au service planification via l'adresse email : serviceplanification@ctguyane.fr ou directement par téléphone au 0594 25 26 37.

Configuration du poste de travail

La collectivité met à disposition d'un utilisateur un poste de travail nécessaire à l'accomplissement de ses fonctions.

L'utilisateur collégien peut installer :

LibreOffice, la suite bureautique : https://fr.libreoffice.org/download/telecharger-libreoffice/

Acrobat Reader DC, logiciel permettant de lire les fichiers PDF : https://get.adobe.com/fr/reader/?promoid=KSWLH

VLC Média player, permettant de regarder des vidéos et d'écouter de la musique et des sons : https://www.videolan.org/vlc/

Deux navigateurs Web, permettant de consulter des pages et des sites Web. Il est recommandé d'en avoir au moins deux sur son PC et sa tablette. En effet, certaines animations et documents sur le Web ne sont pas compatibles avec tous les navigateurs. **Chrome** (conçu par la société Google) **et Firefox** (Mozilla) : https://www.google.com/intl/en_us/chrome/ https://www.mozilla.org/fr/firefox/all/#product-desktop-release

Photofiltre, logiciel de retouches d'images : http://www.photofiltre-studio.com/download.htm ; Version : PhotoFiltre Studio X 10.14.1 (version française avec installeur / 11 Mo)

Autres logiciels :

Scribus: logiciel de PAO (Présentation Assistée par Ordinateur)
XnView: visionneuse d'images avec conversion entre divers formats, application de filtres, capture d'écran, création de vignettes, conversion par lot, diaporama
Audacity: enregistreur et éditeur audio facile d'utilisation et très performant (sait à peu près tout faire)
MathEnPoche: Logiciel d'aide aux élèves, développé par des professeurs de mathématiques en exercice et diffusé par l'association Sésamath
Géogébra: logiciel dynamique de mathématiques réunissant géométrie, algèbre et calcul.
Prezi : logiciel de présentation en ligne avec possibilité de collaboration à distance.
Powtoon : interface en ligne qui permet de créer une vidéo de type "tutoriel", très facilement (idéal pour une recherche ou un exposé).
Google Earth : Partez pour un tour du monde virtuel. Visualisez des bâtiments 3D, des images et des reliefs. Localisez des villes, des adresses et des établissements à proximité.
Framasoft : le site incontournable des Logiciels Libres.
Sweet Home 3D : un logiciel libre d'aménagement d'intérieur qui vous aide à dessiner le plan de votre maison, y placer vos meubles...
SketchUp: logiciel de modélisation 3D convivial et flexible.
Scratch: logiciel libre conçu pour initier les élèves dès l'âge de 8 ans à des concepts fondamentaux en mathématiques et en informatique.
Educlé Collège: Compilation de plus de cent logiciels dédiés aux collégiens.

Vins et Lou: Série d'animation en 15 épisodes permettant de comprendre comment bien surfer en toute sécurité.
GéoPortail 3D: Une cartographie mondiale basée sur les données du projet collaboratif OpenStreetMap.

D'autres informations et applications complémentaires sont inscrites sur le site de la Délégation Académique au Numérique Éducatif (DANE) : https://dane.ins.ac-guyane.fr/

L'utilisateur lycéen peut installer :

Les logiciels issus de ce site : https://doc.ubuntu-fr.org/logiciels_pour_le_lycee

L'URL indispensable pour les collégiens et lycéens :

https://wilapa-guyane.com/auth/saml/wayf?callback=https%3A%2F%2Fwilapa-guyane.com%2F#/

L'utilisateur collégien et lycéen ne doit pas :

- Modifier les équipements et leur fonctionnement, leur paramétrage ainsi que leur configuration physique ou logicielle
- Nuire au fonctionnement des outils informatiques

L'utilisateur doit procéder régulièrement au tri et à l'élimination de ses fichiers « non essentiels » dans le but de préserver la capacité de mémoire et dans le cadre de la mise en jeu de sa responsabilité personnelle en matière de protection des données.

RÈGLES GÉNÉRALES DE SÉCURITÉ ET DÉONTOLOGIE

Authentification sur les postes de travail

L'accès aux ressources informatiques repose sur l'utilisation d'un nom d'utilisateur et mot de passe.
NOM D'UTILISATEUR : ELEVE
MOT DE PASSE : CTG
; fourni à l'utilisateur lors de la remise de cette présente CHARTE par la collectivité. Le mot de passe doit être personnalisé par l'utilisateur dès l'attribution de celui par défaut. Les moyens d'authentification sont personnels et confidentiels.

Tel que préconisé par la CNIL, le mot de passe doit être composé de 12 caractères minimums combinant les caractéristiques suivantes : une majuscule, une minuscule, un chiffre et un caractère spécial. Il ne doit comporter ni le nom, prénom, date de naissance, ni l'identifiant d'ouverture de session, ni suite logique comme « 1234… » ou « azerty… » ou « abcdef… » (qui font partie des listes de mots de passe les plus courants).

Il doit être renouvelé au moins tous les six mois.
Comment créer un mot de passe solide (url disponible et accessible sur le portail des applications) : https://www.cnil.fr/fr/generer-un-mot-de-passe-solide

Votre mot de passe sera indispensable pour chaque connexion sur votre poste. Veuillez à ne pas l'oublier, notez-le si nécessaire.
Exemples :

- la méthode des premières lettres "un tiens vaut mieux que deux tu l'auras" (1tvmQ2tl'A)
- la méthode phonétique "J'ai acheté huit CD pour cent euros cet après-midi" (ght8CD%E7am)

Règles de bonnes pratiques

L'utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service planification toute violation ou tentative de violation suspectée de son compte et de manière générale tout dysfonctionnement ou évènement suspect. Dans le premier cas, un signalement sans délai au DPD est requis
- Ne jamais confier son identifiant/mot de passe à un tiers
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur

- Ne pas stocker ses mots de passe en clair dans un fichier, sur un papier ou dans un lieu facilement accessible par d'autres personnes
- Ne pas utiliser un mot de passe qui serait trop facile à deviner
- Eviter la réutilisation de mots de passe d'une application à l'autre et plus particulièrement entre messagerie personnelle et professionnelle.
- Activer la double authentification lorsque cela est possible
- Ne pas s'envoyer par courriel ses propres mots de passe
- Ne pas masquer sa véritable identité
- Ne pas usurper l'identité d'autrui
- Ne pas modifier les paramètres de son poste de travail
- Ne pas enregistrer ses codes d'accès (Windows, applications, ...) sur les navigateurs
- Verrouiller son ordinateur dès qu'il quitte son poste de travail, même pour un temps limité
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas
- Effectuer des sauvegardes régulières de ses données sur un support externe mis à disposition (disque dur externe, clé USB, etc.)
- Procéder aux tris et « nettoyages » réguliers des données sauvegardées (dans le respect des dispositions du RGPD et du code du patrimoine)

Contrôle parental

Les représentants légaux de l'élève sont chargés de mettre en place le contrôle parental. Pour mieux protéger les enfants sur internet, la loi oblige les fabricants d'appareils connectés (smartphones, tablettes...) à installer un dispositif de contrôle parental et à proposer son activation gratuite lors de la première mise en service de l'appareil. La procédure de mise en place du contrôle parental se trouve en annexe.

Je protège mon enfant : Pour mieux vous informer veuillez consulter la plateforme d'information et d'accompagnement à la parentalité numérique : https://jeprotegemonenfant.gouv.fr/

Usages personnels et scolaires

L'utilisateur doit séparer les usages personnels des usages scolaires :

- Ne pas stocker de données personnelles sur les supports informatiques scolaire
- Eviter de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de la collectivité ; le cas échéant, faire une analyse antivirale complète du support avant l'ouverture d'un fichier présent

Messagerie électronique

Conditions d'utilisation

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par l'éditeur, dans la limite des options et contraintes qu'il établit, notamment :

- Volumétrie de la messagerie
- Taille maximale de l'envoi et de la réception d'un message
- Nombre de destinataires simultanés lors de l'envoi d'un message

Les utilisateurs peuvent consulter leur messagerie à distance, à partir d'équipements privés ou professionnels, à l'aide d'un navigateur (Webmail) ou sur un terminal mobile (smartphone ou tablette).

Contenu de courriels : pièces jointes, liens

Il est strictement interdit à l'utilisateur d'ouvrir des pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que leur envoient habituellement leurs contacts. En cas de doute, il est invité à contacter le service planification : serviceplanification@ctguyane.fr ou directement par téléphone au 0594 25 26 37.

De même, si des liens figurent dans un courriel, il est demandé aux utilisateurs de passer leur souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre. L'utilisateur pourra ainsi vérifier la cohérence de l'adresse.

De façon générale, l'utilisateur doit respecter les règles suivantes :

- Ne jamais répondre par courriel à une demande d'informations personnelles ou confidentielles (par exemple : code confidentiel et numéro de carte bancaire)
- Ne pas ouvrir de pièces jointes ou cliquer sur les liens, sans avoir préalablement vérifié l'adresse de l'expéditeur, la formulation du texte et le bien-fondé de son contenu.
- Ne pas ouvrir et ne pas relayer de messages de type chaînes de lettre, appels à la solidarité, etc.

L'utilisateur doit soigner la qualité des informations envoyées et s'engage à ne pas diffuser d'informations pouvant porter atteinte à l'image de la collectivité, à la dignité humaine, à la vie privée, aux droits et image de chacun ou faisant référence à une quelconque appartenance à une ethnie ou religion.

Internet

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire pour leur activités scolaires.

Toutefois, une utilisation ponctuelle et raisonnable pour un motif personnel des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public et ne met pas en cause l'intérêt et la réputation de l'institution, est admise.

L'utilisateur s'engage lors de ses consultations internet à ne pas se rendre sur des sites « à risque » ou portant atteinte à la dignité humaine (pédopornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes en raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée, etc.).

Pour éviter les abus, l'Autorité Territoriale peut procéder à tout moment au contrôle des connexions entrantes et sortantes et des sites les plus visités (Cass. Soc. 9 juillet 2008 n°06-45-800).

Les systèmes d'information de la collectivité sont protégés par des équipements anti-intrusions malveillantes (Firewall [Pare-feu : matériel dont la fonction est d'assurer la sécurité du réseau], outils de protection de la messagerie, etc.) qui sont mis à jour automatiquement en fonction de l'actualité mondiale des attaques (les url sont classées par catégories : Drug Abuse, Hacking, Illegal, Discrimination, Explicit Violence, Extremist Groups, etc.) et celles qui représentent une menace ou sont sans objet avec l'activité professionnelle sont bloquées.

Les utilisateurs doivent les accepter pour la sécurité du système d'information. Il se peut qu'à ce titre ou pour limiter les engorgements des réseaux, certains accès ne soient pas autorisés ou accessibles.

Téléchargements

En dépit des outils de protection installés sur le matériel informatique, si l'utilisateur télécharge du contenu numérique sur des sites internet dont la confiance n'est pas assurée, il prend le risque d'enregistrer sur son ordinateur des programmes et contenus infectés (virus, cheval de Troie [Logiciel malveillant], etc.).

Afin de veiller à la sécurité de sa machine, de ses données et de celles des autres postes informatiques du parc de la collectivité, l'utilisateur doit respecter les règles suivantes :

- Ne procéder à des téléchargements qu'exclusivement sur les sites de confiance ;
- Décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires n'ayant pas lieu d'être ;
- Rester vigilant concernant les liens auxquels il accède ;
- Privilégier les sites accessibles en « https » ;

Réseaux sociaux et comptes personnels

L'accès aux réseaux sociaux à titre personnel n'est toléré que pour des usages ponctuels.

En tout état de cause, la distinction entre l'utilisation professionnelle et l'utilisation personnelle est requise (création de deux profils). Sur le réseau de données, l'accès aux réseaux sociaux peut être limité voire pour certains inaccessibles en fonction de l'actualité des attaques informatiques et du niveau de sécurité et de risques qu'ils présentent.

Le 3018, un numéro gratuit et une application, pour les victimes de cyberharcèlement

Gratuit, anonyme et confidentiel, accessible de 9 h à 23 h, 7 jours sur 7, le **3018** est le numéro national pour les victimes de violences numériques. C'est le point d'entrée unique pour signaler toute situation de harcèlement et assurer une prise en charge globale et rapide de la victime. Le 3018 traite les signalements de toutes les violences numériques : cyber-harcèlement, « revenge porn», chantage à la webcam, usurpation d'identité, violences à caractère sexiste ou sexuel, exposition à des contenus violents.

Opéré par l'Association e-Enfance dans le cadre du programme Safer Internet de la Commission européenne, son équipe est composée de professionnels, juristes, psychologues et experts numériques.

Le 3018 est désormais joignable 7 jours sur 7, de 9 h à 23 h, par téléphone, sur 3018.fr par tchat en direct, sur les messageries des réseaux sociaux et via l'application 3018.

Le 3018 dispose de procédures de signalement accélérées pour faire supprimer les comptes ou les contenus préjudiciables en quelques heures auprès de plus de 20 plateformes, réseaux sociaux et messageries.

Partenaire du ministère de l'Éducation nationale, du ministère des Sports et des Jeux olympiques et paralympiques, du 119 Enfance en danger, de la plateforme Pharos de la Police nationale, de la Gendarmerie nationale et la Protection judiciaire de la jeunesse (PJJ), il peut réaliser des signalements prioritaires.

Il conseille les victimes dans leurs démarches pour porter plainte, le cas échéant.

Avec l'accord de l'appelant, les signalements faits auprès du 3018 seront transmis aux référents harcèlements académiques pour assurer un suivi immédiat de la situation au sein de l'établissement scolaire.

Téléchargeable sur tous les smartphones (iOS ou Android), l'application 3018 propose 4 fonctions clés :

- La mise en relation directe par tchat ou téléphone avec un professionnel du 3018 ;
- Le stockage des preuves du harcèlement vécu (captures d'écran, photos, liens url, etc.) dans un coffre-fort numérique et sécurisé, ainsi que la possibilité de transférer tout ou partie de ces preuves aux équipes 3018 ;
- Un accès rapide à des fiches pratiques sur le cyberharcèlement pour s'informer sur ses droits et savoir comment réagir ;
- L'auto-évaluation de sa situation à l'aide d'un quiz « Suis-je harcelé ? », pour encourager la victime à demander de l'aide.

Le signalement sera alors transmis aux réseaux sociaux pour qu'ils suppriment en quelques heures les comptes ou les contenus en question, ou bien à la plateforme Pharos, le portail officiel des signalements de contenus illicites sur internet, pour les cas les plus graves.

Plus d'infos sur : https://www.service-public.fr/particuliers/actualites/A15501

Visiteurs, intervenants et prestataires extérieurs

Les visiteurs, intervenants et prestataires extérieurs ne peuvent avoir accès au système d'information de la collectivité (hors réseau wifi « Libre Accès ») sans l'accord préalable du service planification de la Collectivité.

Ils doivent s'engager à respecter la présente charte. Dès lors, les contrats signés entre la CTG et tout tiers ayant accès aux données, aux programmes ou autres moyens informatiques de la collectivité, doivent comporter une clause rappelant cette obligation.

RÈGLES D'UTILISATION DES ÉQUIPEMENTS NOMADES - TRAVAIL À LA MAISON

Equipements Nomades

On entend par « équipements nomades » tous les moyens techniques mobiles informatiques ou de communication (ordinateur portable, tablette, smartphone, clé USB, disque mémoire, clé 4G, etc.).

Ils doivent faire l'objet d'une sécurisation accrue au regard de leur caractère mobile et de la sensibilité des documents qu'ils peuvent contenir. Ces équipements peuvent être mis à disposition des élèves pour un usage strictement scolaire et ne doivent en aucun cas être utilisés par des personnes autre que celle inscrite par l'établissement scolaire et identifié sur le formulaire de prêt de matériel par la Collectivité.

Lorsque ces matériels sont utilisés à l'extérieur de l'établissement scolaire, notamment des vacances scolaires ou week-ends, soit hors des locaux des établissements scolaires, les utilisateurs en assurent la garde et la responsabilité.

En termes de sécurité et de confidentialité, les utilisateurs sont soumis aux mêmes obligations que les utilisateurs restant sur site. Ils devront suivre toutes les prescriptions complémentaires qui leur seront signifiées.

A l'extérieur de l'enceinte scolaire, la connexion à des points d'accès wifi publics qui ne sont pas de confiance (hôtel, gare ou aéroport, etc.) est proscrite.

Les utilisateurs devront se connecter par le biais des clés 3G/4G mis à disposition par la collectivité (via la fonction partage de connexion), ou encore via leur téléphone personnel. L'utilisation de smartphones, ordinateurs portables, ou tablettes, notamment pour la fonction de messagerie électronique comporte des risques particuliers pour la confidentialité des messages et la protection des données, par exemple en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés ils doivent être systématiquement verrouillés.

Les moyens techniques mobiles restitués à la Collectivité sont susceptibles d'être réattribués à d'autres élèves. A cet effet, les utilisateurs s'engagent à supprimer leurs données propres préalablement à leur restitution.

Afin d'assurer la protection des données, la Collectivité s'autorise la prérogative de formater les équipements nomades avant de les réaffecter. En cas de perte ou de vol du matériel, l'utilisateur doit sans délai, le jour du constat, procéder à une déclaration ou une plainte auprès des autorités compétentes (police, gendarmerie, etc.). Il doit également en informer immédiatement le service planification de la direction de l'éducation de la Collectivité afin que les dispositions adéquates soient prises.

Dans le cas où des données professionnelles ou sensibles seraient présentes sur le matériel perdu ou volé, l'utilisateur doit immédiatement en informer la Collectivité qui en informera le DPD.

En cas de dégradation abusive (usage non précautionneux manifeste) du matériel durant sa période de garantie celui-ci ne sera pas remplacé. La collectivité ne pourra être tenue pour responsable en cas de perte de données personnelles intégrées dans les équipements nomades de la collectivité (photos personnelles, messages personnels, etc.).

PROCÉDURES EN CAS DE MOBILITÉ OU DE DÉPART

De façon générale, le matériel informatique et les données professionnelles qu'il contient demeurent au sein de la Collectivité. Cependant, en cas d'accord formalisé par un courrier adressé au service planification de la direction de l'éducation de la Collectivité et entre l'élève, lors de son départ dans les études supérieures le transfert de propriété du poste informatique de l'utilisateur pour acquisition personnelle définitive peut-être acté.

Procédure de départ

Avant son départ dans les études supérieures, l'utilisateur doit les matériels nomades ou de prêts mis à sa disposition. Il doit préalablement en effacer ses fichiers et ses données personnelles.

Les comptes de l'utilisateur (données, messagerie, ...) sont suspendus au départ de l'élève puis supprimés dans un délai d'un mois après le départ.

A ce titre, l'élève devra informer le service planification, au moins deux mois avant l'échéance, de sa date de départ.

En cas de doute sur la nature des données et la conformité au Règlement général pour la protection des données, il est recommandé de saisir le DPD de la collectivité.

SÉCURITÉ DU SYSTÈME D'INFORMATION - PANNE & SAV

Modalités d'intervention pour les pannes et le service après-vente

Le service planification met à disposition les coordonnées pour le SAV du matériel informatique en cas de panne matériel :

ADRESSE DE DEPOT MATERIEL EN PANNE : LOT COLLERY II 97300 CAYENNE
TEL : 05 94 31 31 34
INFORMATION A TRANSMETTRE :

- Marque : LENOVO
- Article : PC PORTABLE
- N° de Série : inscrit au dos au pc portable
- N° client : C0000017

Les pannes logicielles ne sont pas prises en compte dans le cadre du SAV. Ces types de pannes sont exclusivement imputables aux divers programmes installés sur l'ordinateur. L'élève peut se rapprocher de l'informaticien présent au

sein de son établissement scolaire pour un diagnostic. Si impossibilité l'élève devra alors faire diagnostiquer son équipement par une entreprise informatique certifiée. Les frais de réparation sont à la charge de l'élève.

Pour toutes autres demandes contacter par email : serviceplanification@ctguyane.fr

Accès au poste de travail

A des fins d'interventions ou de maintenance informatique, la Collectivité peut accéder aux postes de travail. Dans le cadre de mises à jour et évolutions du système d'information ou pour la gestion centralisée de paramètres. La Collectivité peut être amenée à intervenir sur l'environnement technique des postes de travail sans jamais intervenir sur les contenus.

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

La CTG dispose d'un Délégué à la Protection des Données (DPD ou DPO [Data Protection Officer]).

Le Règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et communément appelé Règlement Général sur la Protection des Données (RGPD) est entré en vigueur le 25 mai 2018. Le RGPD vient modifier la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa version initiale ; il impose les conditions dans lesquelles des traitements de données à caractère personnel peuvent être réalisés. Cette règlementation ouvre aux personnes concernées par les traitements un droit d'information, d'accès, de rectification, d'effacement, de portabilité et d'opposition des données personnelles les concernant.

Les utilisateurs doivent veiller :

- À respecter l'intégrité et la confidentialité des données, tant pour la collecte, le traitement et la communication interne et externe des données,
- Ne pas collecter des données qui, en raison de leur contenu, contreviendraient aux lois et règlements en vigueur.

Le représentant de la collectivité est responsable de traitement au titre du RGPD, c'est lui qui détermine les finalités et les moyens du traitement et qui décide de sa mise en œuvre. A ce titre, il en assume la responsabilité.

Les données sont collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

Le RGPD impose à tous les organismes privés et publics de désigner un délégué à la protection des données pour faciliter la conformité avec les dispositions du RGPD.

Depuis le 27 novembre 2018, la collectivité a désigné un Délégué à la protection des données à caractère personnel auprès de la CNIL (n° DPO – 35214).

Les missions du DPO sont listées à l'article 39 du RGPD.

Ce dernier a entre autres pour mission :

- D'informer et conseiller le responsable du traitement ou le sous-traitant ainsi que leurs agents et employés des obligations qui leur incombent en vertu du RGPD et de l'ensemble de la législation nationale, européenne et internationale en matière de protection, de sécurisation et de transfert des données,
- De veiller à la conformité des mesures techniques et opérationnelles mises en œuvre par le responsable de traitement afin de se conformer au RGDP et aux mesures de sécurité mises en œuvre,
- De contrôler le respect du présent règlement, etc.

Il est obligatoirement consulté par l'ensemble des élèves préalablement à la création d'un traitement de données à caractère personnel, et pour la mise en conformité des traitements existants. Le délégué à la protection des données accompagne l'ensemble des services à la mise en conformité ou à l'élaboration d'une étude d'impact notamment pour le traitement de données sensibles au sens du RGPD.

L'article 30 du RGPD impose au responsable de traitement de tenir un registre des activités de traitements afin de disposer d'une vue d'ensemble du traitement des données à caractère personnel au sein de la collectivité et des mesures de sécurité qui sont mises en œuvre.

Ce document de recensement et d'analyse participe à documenter la conformité. Le délégué à la protection des données collabore à ce recensement avec l'ensemble des services de la collectivité au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande. Elle est également diffusée sur l'intranet de la Collectivité.

Le Délégué à la protection des données veille au respect des droits des personnes concernées. Elles disposent de droits afin de garder la maitrise de leurs données.

Les principaux droits sont les suivant : droit à l'information, recueil du consentement, droit d'accès, de rectification, d'opposition, droit à la portabilité, à l'effacement, etc. Lorsque ces droits sont exercés, les personnes doivent obtenir une réponse dans un délai d'un mois. En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le DPD à l'adresse dpd@ctguyane.fr

RESPONSABILITÉS ET SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.

Le non- respect de la présente charte peut entrainer une limitation des accès au système d'information de la CTG de la personne concernée.

Des sanctions peuvent être prononcées. Elles consistent :

- Dans un premier temps, en un rappel à l'ordre émanant de l'établissement scolaire ou de la Collectivité après avis du Directeur général des services en cas de non-respect des règles énoncées par la charte ;

- Dans un second temps et en cas de renouvellement, en une sanction disciplinaire adoptée selon la procédure statutaire en vigueur.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information (cf. liste des textes en annexe) est susceptible de sanctions pénales par la loi.

ENTRÉE EN VIGUEUR DE LA CHARTE

La présente charte entre en vigueur dès sa signature par les élèves et leurs représentants légaux.

Elle a été présentée pour avis du Délégué à la protection des données de la CTG.

Toute actualisation sera portée à la connaissance des parties prenantes.

ANNEXES

DISPOSITIONS LÉGALES APPLICABLES

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiées par la loi n°2004-801 du 6 août 2004, dans sa version consolidée du 14 juin 2018.

Règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, entré en vigueur le 25 mai 2018 (RGPD).

Dispositions Pénales :

- Code Pénal (partie législative) : art 226-16 à 226-24 ;
- Code Pénal (partie réglementaire) : art R.625-10 à R.625-13 ;
- Loi n°88-19 du 5 janvier 1988 à la fraude informatique dite loi Godfrain. Dispositions pénales : art 323-1 à 323-3 du Code Pénal ;
- Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels. Disposition pénale : art L.335-2 du Code Pénal.

ACTIVER LE CONTROLE PARENTAL

Pour **configurer** le contrôle parental sur un PC Windows 11, vous devez :

- Configurez un compte enfant sous Windows 11
- Ouvrez l'application **Paramètres** sous Windows 11.
- Ensuite, appuyez sur l'onglet **Comptes** disponible dans le volet de gauche.
- Sélectionnez la section **Famille et autres utilisateurs** dans la liste.

Pour **configurer** les filtres de contrôles parentaux, vous devez :

La prochaine partie consiste à configurer effectivement les paramètres de contrôle parental. Voici comment procéder :

1- Appuyez les touches **Windows + I** sur votre clavier pour accéder directement aux Paramètres.
2- Rendez-vous à la section Comptes, Famille et autres utilisateurs, puis sélectionnez l'option **Gérer les paramètres familiaux en ligne ou supprimer un compte**.
3- Vous serez dirigé vers la page correspondante à Microsoft Family Safety dans votre navigateur.

Lien complet : https://windowsreport.com/fr/windows-11-controle-parental/

Pour **activer** le contrôle parental sur un PC Windows 11, vous devez :

1- Créer un compte Microsoft pour votre enfant.
https://lecrabeinfo.net/comment-creer-un-compte-microsoft.html
2- Inviter votre enfant à rejoindre le groupe familial de Microsoft Family Safety (c'est ici que vous contrôlerez son activité).
3- Demander à votre enfant (vous pouvez le faire vous-même) d'accepter l'invitation à rejoindre le groupe familial.
4- Ajouter un nouvel utilisateur « enfant » sur le PC Windows 11 avec le compte Microsoft de votre enfant.
5- Vous serez redirigé vers cette page : https://www.microsoft.com/fr-fr/microsoft-365/family-safety pour configurer les règles de contrôle parental à appliquer.
Voici à quoi s'attendre quant aux divers onglets et options proposées sur la page Sécurité familiale :
   - **Temps d'utilisation** (Les options Temps d'écran et **Utiliser un calendrier** vous permettront de configurer les limites de temps d'écran sur tous les appareils).
   - Filtrage de contenu (L'option **Filtrer les sites Web et les recherches inapproprié** bloquera le contenu réservé aux adultes au niveau du compte de l'enfant. D'autres options intéressantes sont également disponibles dans cette section telles que **Utiliser uniquement les sites Web autorisés, Applications et jeux** pour permettre uniquement les applications et les jeux soumis à une limite d'âge et plus encore).
   - Résumés sur l'activité (Cette option vous permettra de surveiller l'activité Web déroulée sur le compte de votre enfant).
   - Dépenses (Option qui sert à vérifier les méthodes de paiement autorisées, recevoir des notifications sur les achats en ligne effectués par votre enfant ou restreindre ces opérations complètement).

Lien complet : https://lecrabeinfo.net/windows-11-activer-le-controle-parental-family-safety-pour-un-enfant.html

RÉFÉRENCES / COORDONNÉES

Direction de l'éducation enseignement supérieur – Service Planification de la CTG.

- Site Cité Administrative Territoriale : Bâtiment A – Carrefour de Suzini 4179, Route de Montabo – 97307 CAYENNE (**0594 25 26 37**

DPD (Déléguée à la Protection des Données) : Madame Mylène ELI

- Cité Administrative Territoriale – Bâtiment A – Tél. fixe : **0594 28 96 04**
  Courriel : dpd@ctguyane.fr

SIGNATURE ET ENGAGEMENT

Je confirme avoir pris connaissance des informations mentionnées dans cette présente Charte **le** :

DATE :

VILLE :

ETABLISSEMENT SCOLAIRE DE RATTACHEMENT :

SIGNATURE DE L'ELEVE DESTINATAIRE DU MATERIEL, suivi de la mention « Lu et approuvé » :

SIGNATURE REPRESENTANT LEGAL DE L'ELEVE, suivi de la mention « Lu et approuvé » :

Le Président de la Collectivité Territoriale de Guyane