

The background is a dynamic, abstract composition of numerous thin, flowing lines in shades of blue, cyan, and magenta, with some brighter orange and yellow highlights. These lines create a sense of movement and depth, resembling a digital or data landscape.

CHARTRE DU NUMÉRIQUE, DE L'INFORMATIQUE ET DE LA TÉLÉPHONIE

TABLE DES MATIÈRES

I	Préambule	4
II	Glossaire	5
III	La sécurité	6
IV	Matériels	7
	A - Postes de travail	7
	B - Périphériques	7
	C - Téléphonie	8
	D - Restitution	8
	E - Réseaux	9
	F - Logiciels/progiciels	9
V	Netiquette	10
	A - Réseaux Sociaux	10
	B - Internet	10
	C - Messagerie	10
VI	RGPD	12
VII	Synthèse des pistes d'amélioration pour une utilisation plus écoresponsable	13
	Annexe 1	14
	Annexe 2	14
	Annexe 3	15

I – PRÉAMBULE

L'informatique, les réseaux et les télécommunications se sont particulièrement développés ces dernières années au sein des administrations. Le renfort en équipements matériels, les nouveaux outils logiciels déployés ont permis d'améliorer l'efficacité des services et, par certains aspects, les conditions de travail. Pour accompagner cette modernisation, il est important de mettre en place un ensemble de moyens destinés à pérenniser et à sécuriser les systèmes d'information.

La présente charte a pour but de fixer les règles d'utilisation des outils de communication dans l'intérêt des utilisateurs et de la collectivité. Ces règles concernent les ordinateurs, les logiciels de messagerie, la navigation sur Internet, et la téléphonie.

L'utilisation de tout système de communication suppose de la part des utilisateurs, le respect de règles dont le rôle est d'assurer la sécurité, les performances des traitements, la préservation des données confidentielles et personnelles ainsi que l'émission et la réception de données dans le respect des législations applicables.

Cette charte 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. L'imprudence, la négligence ou la malveillance d'un utilisateur peut en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de la collectivité.

Chaque utilisateur de la collectivité doit contribuer, à son niveau, à la protection des ressources informatiques, en mettant en application des règles de bon sens et en appliquant les recommandations fournies par la Direction des Systèmes d'Information (DSI).

La présente Charte a également pour objet de rappeler les types d'outils informatiques mis à disposition et de mettre en place des règles de bon usage de ces outils. Elle s'appliquera à tout le personnel travaillant de façon permanente ou temporaire à la Mairie de Petit-Quevilly, au CCAS, et à la Caisse des Écoles (à savoir : titulaire, contractuel, stagiaire, collaborateur bénévole, agent sous statut privé...), ainsi que les élus. Cette charte a été soumise au comité social territorial du 14 novembre 2023

II - GLOSSAIRE

Client léger : équipement informatique ne contenant aucune application, qui permet uniquement de se connecter sur un serveur sur lequel seront exécutées toutes les applications de l'utilisateur.

Courriel/mail/mél : courrier électronique

Data Center : centre de traitement des données qui rassemble des équipements d'un système d'information organisé en baies et armoires (serveurs, ordinateurs, équipements réseaux et télécommunications).

DPD : Délégué à la Protection des Données.

Logiciel : ensemble des programmes et des procédures nécessaires au fonctionnement d'un système informatique. Programme informatique.

Moteur de recherche : système matériel et logiciel permettant de trouver des informations sur Internet (pages web, images, vidéos, forums, blogs...) à partir de mots clés.

Navigateur web : logiciel permettant de consulter les contenus d'un serveur web ou d'un logiciel web

Netiquette : règles de savoir-vivre en usage sur internet et sur la messagerie.

Pare feu ou coupe-feu : il s'agit d'un dispositif informatique qui filtre les flux d'informations (les paquets) entre un réseau interne à un organisme et le réseau externe (Internet) en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur. Traduction anglaise : Firewall.

Pourriel/spam : courrier électronique indésirable, envoyé massivement aux utilisateurs.

Progiciel : ensemble de programmes conçus pour être fournis à différents utilisateurs en vue d'une même application ou d'une même fonction.

Réseau : tout équipement permettant de relier entre elles les ressources informatiques.

RGPD : Règlement Général pour la Protection des Données et désigne la dernière directive européenne concernant les données personnelles.

Serveur : dispositif informatique qui offre des services à un ou plusieurs utilisateurs.

URL : adresse web à utiliser dans un navigateur web.

III – LA SÉCURITÉ

La sécurité informatique consiste à assurer l'utilisation des ressources matérielles ou logicielles de la collectivité uniquement dans le cadre prévu.

Tout utilisateur est responsable de l'usage des ressources auxquelles il a accès et doit contribuer, à son niveau, à la sécurité générale des moyens mis à sa disposition.

Il s'engage donc à ne pas effectuer des opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau et sur l'intégrité de l'outil informatique.

L'utilisation des ressources doit être rationnelle et loyale afin d'éviter la saturation ou leurs détournements à des fins personnelles.

Un utilisateur ne doit pas installer sur le réseau local ou sur sa machine des logiciels susceptibles de contourner ou d'affaiblir les dispositifs de sécurité.

Afin de protéger le Système d'Information, la Direction des Systèmes d'Information (DSI) a mis en place un Anti-virus sur chaque poste dont les mises à jour se font automatiquement, et système Anti-spam, permettant aux utilisateurs de ne pas recevoir de communications électroniques massives et un filtrage d'accès internet, protégeant le réseau de la collectivité contre les intrusions et l'accès aux catégories de sites web illégaux, inappropriés aux missions de service public.

Néanmoins ces dispositifs ne peuvent garantir à 100 % et ne protègent pas la confidentialité des données circulant sur le réseau, il appartient donc à l'agent de rester vigilant.

Les ressources informatiques, les services internet, la téléphonie et autres moyens de télécommunications sont utilisés exclusivement pour l'activité professionnelle.

L'utilisateur est tenu, dès qu'il a connaissance de tout incident de sécurité (apparition de virus, tentative d'intrusion ou intrusion) et de manière générale de tout dysfonctionnement qu'il serait amené à observer, d'éteindre son poste de travail et de le signaler à un ambassadeur sécurité informatique, à son responsable hiérarchique et à la Direction des Systèmes Informatiques.



Pictogramme identifiant les informations relatives à la sécurité informatique contenues dans la présente charte.

IV - MATÉRIELS

A - Postes de travail

Standard	Mobile
• Un client léger ou une unité centrale • Un ou deux écrans • Un clavier • Une souris	• Un ordinateur portable • Un écran • Une souris

En cas d'absence momentanée, l'utilisateur doit verrouiller son PC :

Pour un verrouillage rapide 	Pour un verrouillage classique Ctrl + Alt + Suppr puis cliquez sur <i>Verrouiller l'ordinateur</i>
--	---

Chaque utilisateur est doté d'un identifiant et d'un mot de passe. Ceux-ci sont strictement personnels et ne doivent en aucun cas être communiqués (ni notés sur des supports accessibles à autrui). Leur saisie devra se faire à l'abri des regards. Le mot de passe devra également être changé régulièrement (6 mois maximum), ou si vous pensez que quelqu'un d'autre a pu en prendre connaissance.

Le mot de passe doit faire au minimum 12 caractères et doit contenir au moins :

- 1 lettre en majuscule,
- 1 lettre en minuscule,
- 1 chiffre,
- 1 caractère spécial (!,;,:&()\$).

Pour changer son mot de passe Ctrl + Alt + Suppr puis cliquez sur <i>Modifier un mot de passe</i>
--

En cas d'absence prolongée et/ou imprévue, la DSI pourra réinitialiser le mot de passe et le transmettre au chef de service afin d'assurer la continuité des missions.

B - Périphériques

- Webcam
- Clé USB, Clé de signature électronique
- Systèmes d'impression (copieur/scan/imprimante)
- Scanner
- Imprimante

À la fin de sa journée de travail, l'utilisateur doit fermer ses logiciels, sa session et éteindre son pc, son écran et les systèmes d'impression s'il est le dernier à partir.



En 2020, des collectivités comme les nôtres réalisent environ 1500 000 copies/impressions. L'activation du mode recto/verso permettrait un gain de 750 000 feuilles soit l'équivalent de 94 arbres.

500 impressions, c'est en moyenne 6 % d'un arbre, 8.5 kW, 10 litres d'eau.

- ✓ Imprimez les documents confidentiels sur les systèmes d'impression partagés en mode « impression privée ».
- ✓ Travaillez dans la mesure du possible à l'écran pour limiter l'usage papier, par exemple en utilisant la séparation d'écran.
- ✓ Conservez le paramétrage par défaut noir et blanc et recto/verso.
- ✓ Utilisez l'aperçu avant impression pour éviter les erreurs.

LE SAVIEZ-VOUS ?

1/4 des impressions sont jetées dans les 5 minutes suivant l'impression.

C - Téléphonie

- Un GSM ou un smartphone
- Un téléphone fixe
- Un casque

Par respect d'autrui, le smartphone ne doit pas venir perturber une réunion ou un entretien. Privilégiez le mode vibreur ou silencieux. Si vous devez prendre l'appel, sortez de la salle.

Les appels vers des numéros internationaux, spéciaux (118 XXX, 3635, etc.) et/ou surtaxés sont à éviter dans la mesure du possible (privilégiez par exemple la recherche d'un numéro de téléphone sur un site d'annuaire gratuit et bannissez la mise en relation).

Pour des raisons de sécurité, le matériel informatique ne doit pas être laissé à la vue ou à la disposition de toute personne en dehors de la collectivité (Ex. : ordinateur sur le siège passager d'une voiture...).

D - Départ de la collectivité

En cas de départ définitif de la collectivité, d'un changement d'affectation, ou d'attribution d'un nouveau matériel, l'utilisateur devra obligatoirement **remettre à la DSI les matériels mobiles** (téléphone, PC portable, Smartphone, tablette, etc.) dont il n'a plus l'usage, afin d'être réattribués.

Le responsable de l'agent partant devra informer la DSI via le formulaire « fermeture compte utilisateur ».

E - Réseaux

Sur le réseau des emplacements spécifiques (espaces de stockage) sont mis à disposition :

- [Nom d'utilisateur](Z:) est un espace de stockage personnel sur le réseau : seul l'utilisateur peut y accéder,. Des sauvegardes automatiques sont réalisées pour permettre une restauration des fichiers en cas de nécessité,
- un espace de stockage réservé à votre service

Des espaces de stockage partagés par service sont disponibles soit automatiquement ou l'utilisateur a la possibilité des les ajouter en fonction des ses droits. Ces ressources sont accessibles depuis ce chemin :

\\petit-quevilly.fr\mairie\...

☒ *Privilégiez de sauvegarder vos documents sur les espaces de stockage en réseau car ceux-ci sont sauvegardés quotidiennement contrairement au disque dur du Poste de travail (par exemple « Mes documents » ou le Bureau) qui lui, n'est pas sauvegardé.*

☒ *Évitez de sauvegarder ou enregistrer plusieurs fois le même document à des emplacements différents pour ne pas surcharger l'espace de stockage sur le réseau.*

 **Il est interdit de raccorder sur le réseau tout type d'équipement non mis à disposition par la DSI, sans son autorisation.**

F - Logiciels/Progiciels

Des logiciels de base sont mis à disposition par la DSI:

- Traitement de texte
- Tableur
- Lecteur de PDF
- Navigateur
- ...

Les progiciels spécifiques à chaque service sont installés par la DSI.

En cas de besoin, vous pouvez demander à la DSI, l'installation d'autres logiciels/progiciels gratuits ou si ceux-ci sont payants, en faire la demande lors de la préparation budgétaire.

En tout état de cause vous ne devez pas installer et/ou utiliser de logiciel dont la collectivité n'est pas en possession d'un droit d'usage gratuit ou payant.

L'ensemble des logiciels et progiciels utilisés au sein des collectivités sont listés en annexe 1.

 **Pour des nécessités de sécurité, de maintenance, de gestion technique et de bon usage, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle du responsable informatique et de l'autorité territoriale, être analysés et contrôlés dans le respect de la législation applicable.**

V - NETIQUETTE

A - Réseaux Sociaux

Tout agent est soumis à un devoir de neutralité, discrétion, secret professionnel et d'obligation de réserve. L'utilisation d'Internet et des réseaux sociaux, **y compris en dehors du temps de travail**, devra satisfaire ces obligations.

B - Internet

Comme le prévoit la loi, l'utilisateur s'engage à ne pas se rendre sur des sites illégaux (portant atteinte à la dignité humaine, incitation à la haine...).

L'utilisateur ne doit pas également se rendre sur des sites inappropriés dans le cadre professionnel (jeux et paris en ligne...).

Un système de blocage est mis en place par la collectivité afin d'empêcher l'accès à la majorité de ces sites.

Le téléchargement, en tout ou partie, de données numériques soumises au droit d'auteur ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.

Il est interdit de communiquer une image ou sa reproduction au public sans autorisation préalable du ou des auteurs.

Dans une finalité de sécurité de son système d'information, l'utilisateur est expressément informé que la ville de Petit-Quevilly se réserve le droit de surveiller à tout moment l'utilisation faite des services internet et d'y opérer une trace.

Un système de filtrage web contrôle les consultations afin de garantir et de protéger la collectivité et ses agents pendant l'utilisation et les consultations internet en fonction de profils prédéterminés.

C - Messagerie

Remplacez au maximum les pièces jointes par un lien hypertexte ou URL. Pour les documents très lourds, pensez aux dossiers de partage de la collectivité et pour les envois à l'extérieur de la collectivité les outils de type Google Drive ou WeTransfer.

L'utilisateur veillera à ne pas ouvrir les courriels dont le sujet paraîtrait suspect (message écrit en anglais ou autre, destinataire inconnu...) et en informera son ambassadeur sécurité informatique et la DSI.

L'utilisateur devra éviter de mettre en destinataire des personnes qui ne sont pas concernées par le mail envoyé pour ne pas créer de pourriels. De même, il devra utiliser la fonction « répondre à tous » uniquement quand cela est nécessaire.

LE SAVIEZ-VOUS ?

Envoyer un mail de 1 Mo (donc avec une pièce jointe) équivaut à 1 heure d'utilisation d'une ampoule de 25 W.



Les emails d'une entreprise de 100 personnes génèreraient 18 tonnes d'équivalent CO₂ par an, soit l'équivalent de 18 allers-retours Paris/New York.

L'utilisateur devra veiller à utiliser de manière pertinente les champs servant à indiquer le destinataire d'un mail.

À...	
Cc...	
Cci...	

- "À" est l'emplacement destiné à saisir l'adresse du ou des destinataires principaux dont on attend une action ou une réponse. Il est visible de tous.
- "Cc" ou "copie carbone" permet de distinguer les destinataires principaux des destinataires secondaires. L'usage veut que l'on adresse un mail en "Cc" aux contacts dont on n'attend pas de réponse ou d'action directe.
- "Cci" signifie "Copie Carbone Invisible". C'est le champ correct à utiliser quand on veut envoyer une "copie cachée". Les adresses des destinataires inscrits en "Cci" n'apparaissent pas dans le mail reçu par les autres destinataires. On s'en sert essentiellement pour protéger l'anonymat de ses correspondants.
- Ne pas oublier d'indiquer un objet explicite au message, cela améliore la lisibilité pour le destinataire, et évite à votre message d'être considéré comme un spam voire d'être bloqué par les systèmes de sécurité

L'utilisateur devra respecter la charte graphique en vigueur (couleurs d'écriture, pavé de signature, ne pas saisir le corps du message en majuscules...).

L'utilisateur doit éviter de surcharger l'espace de stockage du serveur de messagerie. Les messages importants sont à conserver et/ou archiver, les autres à supprimer. Le dossier « éléments supprimés » doit être vidé périodiquement.

LE SAVIEZ-VOUS ?

Un mail stocké, c'est 10 g de CO₂ par an.

Tout courrier électronique ne portant pas la mention « personnel et confidentiel » ou « privé » dans son objet sera considéré comme professionnel et pourra donc être ouvert par l'Autorité territoriale ou le référent informatique, afin d'assurer la continuité de service.



Hors personnel soumis à nécessités de service, tous les agents ont le droit à la déconnexion et n'ont pas à répondre aux courriels et autres messages en dehors de leur temps de travail, afin de garantir l'équilibre entre vie professionnelle et vie privée, et réduire les risques psychosociaux.

VI - RGPD

Les principaux objectifs du Règlement Général pour la Protection des Données sont d'accroître à la fois la protection des personnes concernées par un traitement de leurs données à caractère personnel et la responsabilisation des acteurs de ce traitement.

Les obligations des collectivités sont :

CONSTITUER UN REGISTRE DE TRAITEMENTS DES DONNÉES



RESPECTER LES DROITS DES PERSONNES



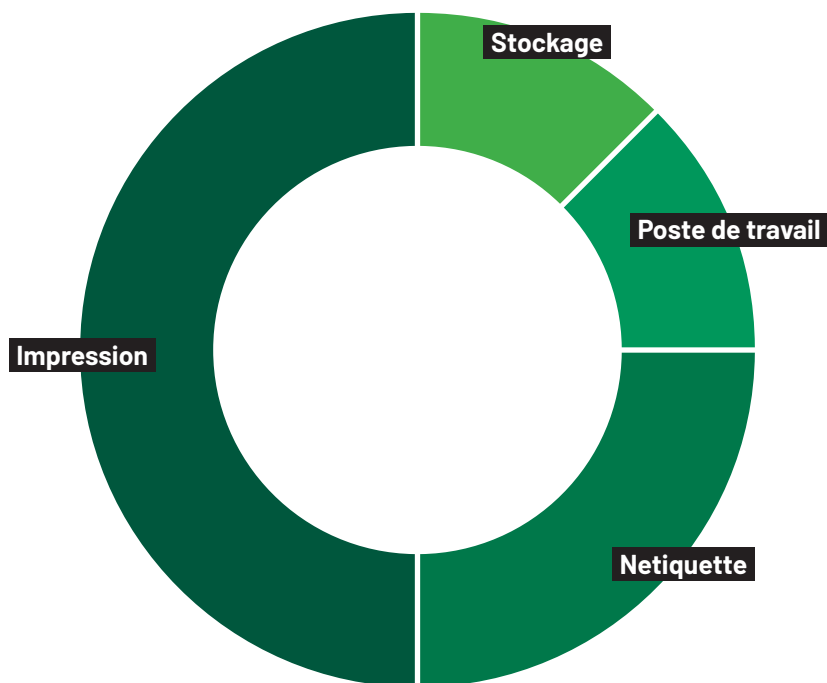
SÉCURISER LES DONNÉES



Toute personne susceptible de manipuler des données à caractère personnel devra vérifier auprès de la personne concernée si celle-ci en a autorisé son utilisation.

Cette réglementation s'applique autant aux données dématérialisées (logiciel, fichier, message) que sur des supports physiques.

VII – SYNTHÈSE DES PISTES D'AMÉLIORATION POUR UNE UTILISATION ÉCORESPONSABLE



**Soyez participatif et acteur afin d'améliorer ensemble
l'impact de nos collectivités sur l'environnement !**

ANNEXE 1 : LES LOGICIELS / PROGICIELS GRATUITS / PAYANTS

Logiciels gratuits	Logiciels payants
Google Chrome PDF24 Adobe Reader Gantt Project Java PlayerFlash Player Gimp Freeplane One note Libre Office	Word Excel Powerpoint Outlook Suite Adobe Creative Cloud Autodesk TeamViewer

Progiciels	
Gestion État Civil Gestion du cimetière Gestion des marchés Gestion financière Gestion Ressources humaines Gestion des Actes Gestion des courriers Parapheur électronique	Gestion Technique Gestion du temps et badgeage Kiosque famille Gestion Piscine Gestion École de musique Gestion des élections Gestion de l'instruction des Sols Suivi des alerte PCS

ANNEXE 2 : LES LIENS UTILES

Pour accéder à l'internet de la mairie :

<http://intranet.petit-quevilly.fr>

Pour réaliser des demandes d'intervention auprès de la DSI :

<http://ticket.petit-quevilly.fr/>

Pour réaliser des demandes d'intervention auprès de la DT :

<https://interventions.petit-quevilly.fr/>

Site de la mairie de Petit-Quevilly :

<https://www.petit-quevilly.fr/>

Site du conseil départemental de Seine-Maritime :

<https://www.seinemaritime.fr/>

Site de la préfecture de Seine-Maritime

<https://www.seine-maritime.gouv.fr/>

CATÉGORIE	MAIRIE	PUBLIC
RISQUE PÉNAL		
Stupéfiants	⚠	✗
Piratage	⚠	✗
Illégal ou non-éthique	⚠	✗
Discrimination	⚠	✗
Violence	⚠	✗
Groupes extrémistes	⚠	✗
Évasion par proxy	⚠	✗
Plagiat	✗	✗
Abus sexuel d'enfant	✗	✗
Terrorisme	✗	✗
Extraction de crypto-monnaie	✗	✗
Programme potentiellement indésirable	✗	✗
ADULTE/CONTENU MATURE		
Croyances alternatives	✗	✗
Avortement	✗	✗
Contenu adulte	✗	✗
Groupe de pression, lobbies	✗	✗
Paris et jeux	✗	✗
Nudité	✗	✗
Pornographie	✗	✗
Site de rencontre	✗	✗
Armes (vente)	✗	✗
Marijuana	✗	✗
Éducation sexuelle	✗	✗
Alcool	✗	✗
Tabac	✗	✗
Lingerie et maillot de bain	✗	✗
Chasse et jeux de guerre	✗	✗
CONSOMMATEUR DE BANDE PASSANTE		
Téléchargements de logiciels	✓	✗
Partage et stockage de fichiers	✓	✓
Streaming et téléchargements	✓	✗
Partage de fichiers en peer-to-peer	✓	✗
Internet radio et TV	✓	✗
Téléphonie sur internet	✓	✓

CATÉGORIE	MAIRIE	PUBLIC
RISQUE DE SÉCURITÉ		
Site web malveillant	⊗	⊗
Hameçonnage	⊗	⊗
URL de spam	⊗	⊗
DNS dynamique	⊗	⊗
Domaine nouvellement observé	⊗	⊗
Domaine nouvellement enregistré	⊗	⊗
INTÉRÊT GÉNÉRAL - PERSONNEL		
Publicité	✓	✓
Change et transaction	✓	⊗
Jeux	⊗	⊗
Messagerie web	✓	✓
Divertissements	✓	✓
Arts et culture	✓	✓
Éducation	✓	✓
Santé et bien-être	✓	✓
Recherche d'emploi	✓	✓
Médicaments	✓	✓
Actualités et médias	✓	✓
Réseaux sociaux	✓	✓
Organisations politiques	✓	✓
Références	✓	✓
Religion	⊗	⊗
Achats	✓	✓
Hobbies	✓	✓
Sports	✓	✓
Voyages	✓	✓
Véhicules	✓	✓
Serveur de contenu dynamique	✓	✓
Sans contenu	✓	✓
Folklore	✓	✓
Chat web	✓	✓
Messagerie instantanée	✓	✓
Forums de discussion	✓	✓
Cartes postales digitales	✓	✓
Éducation enfantine	✓	✓
Immobilier	✓	✓
Restaurants	✓	✓
Sites web personnels et blogs	✓	✓
Serveurs de contenu	✓	✓
Nom de domaine réservé	✓	✓
Privé et personnel	✓	✓
Enchères	✓	✓

CATÉGORIE	MAIRIE	PUBLIC
INTÉRÊT GÉNÉRAL - COMMERCE		
Finance et banques	✓	✓
Moteur de recherche et portails	✓	✓
Organisation générale	✓	✓
Économie, affaires	✓	✓
Sécurité informatique	✓	✓
Organisme public	✓	✓
Technologies de l'information	✓	✓
Forces armées	✓	✓
Hébergement web	✓	✓
Sites web sécurisés	✓	✓
Applications web	✓	✓
Organisme de bienfaisance	✓	✓
Accès à distance	✓	✓
Analyse de données web	✓	✓
Rencontre en ligne - visio/teams	✓	✓
Raccourcissement d'URL	✓	✓

LES BONS RÉFLEXES POUR ÊTRE UN AGENT NUMÉRIQUE RESPONSABLE



J'ÉTEINS

mon poste de travail
le soir & je ne donne
JAMAIS mon mot de
passe



JE VÉRIFIE TOUJOURS

la provenance des
mails que je reçois



JE VÉRROUILLE

mon poste de travail
quand je m'absente



SI

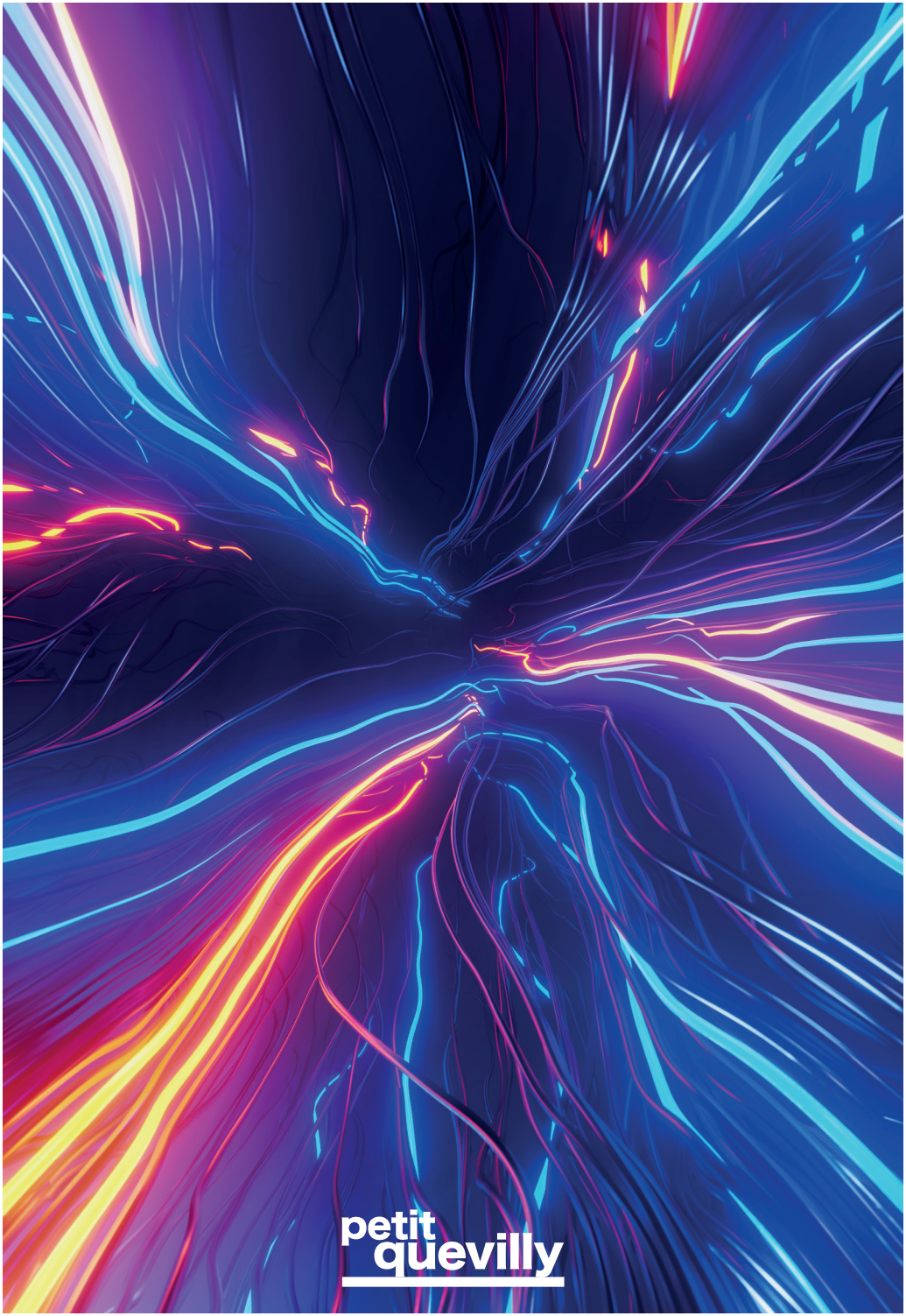
mon ordinateur
fonctionne
anormalement
JE L'ÉTEINS
JE LE DÉBRANCHE
JE CONTACTE LA DSI



SI

mon mot de passe
ne contient pas
12 caractères
JE LE CHANGE
CTRL + ALT + SUPPR





petit
quevilly