CHARTE INFORMATIQUE

Dans le cadre de son activité, IXAD, (ci-après, « **IXAD** ») met son système d'information, y compris son réseau informatique et téléphonique, et les différents matériels numériques (ci-après désignés ensemble les « **Outils Numériques** ») à la disposition des salariés autorisés par IXAD à les utiliser et de ses collaborateurs (ci-après désignés ensemble les « **Utilisateurs** ») pour l'accomplissement de leurs missions.

La présente charte (ci-après, la « **Charte** ») vise à définir :

- Les modalités d'accès et les conditions d'utilisation des Outils Numériques mis à la disposition des Utilisateurs afin d'assurer un niveau optimum de sécurité, de confidentialité des données et de performance du système d'information et, de manière générale, le respect des dispositions légales et règlementaires en vigueur ;

- Les moyens de contrôle et de surveillance de l'utilisation des Outils Numériques ;

- Les droits et devoirs des Utilisateurs.

La Charte vise, en outre, à **sensibiliser les Utilisateurs aux cyber-risques** et à contribuer à assurer la sécurité des Outils Numériques. Ces risques doivent être appréhendés en respectant des règles de sécurité et des « bonnes pratiques » inhérentes à la sécurité des Outils Numériques que tous les Utilisateurs s'engagent à respecter.

Cette Charte fait de **l'Utilisateur un acteur essentiel de la réalisation de ces objectifs**. Il incombe aux Utilisateurs de faire un usage raisonné et raisonnable des Outils Numériques mis à leur disposition et de respecter des obligations générales telles que la confidentialité, la discrétion ou encore la vigilance.

Ainsi, chaque Utilisateur s'engage à ne pas faire preuve d'imprudence, de négligence ou de malveillance à l'égard des Outils Numériques, sous peine d'engager sa responsabilité civile et/ou pénale ainsi que celle de IXAD.

Dans le cadre de la réforme du droit des données à caractère personnel et notamment au regard des dispositions du Règlement européen n°2016/679 du 27 avril 2016 (ci-après, le « **Règlement** »), entré en application le 25 mai 2018, IXAD a souhaité adopter de nouvelles mesures afin **d'assurer sa conformité au nouveau droit applicable et de définir une véritable politique de protection et de sécurité des données.**

Aux termes de la règlementation applicable, **constitue une donnée à caractère personnel** :

« *toute information se rapportant à une **personne physique identifiée ou identifiable** (ci-après dénommée **« Personne concernée »**) ; est réputée être une « personne physique identifiable », une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Ainsi, le nom de famille, le prénom, l'adresse électronique, le numéro de téléphone, le numéro de sécurité sociale ou le numéro d'une carte de paiement d'une personne physique constituent des données à caractère personnel.

La Charte s'inscrit dans une démarche de protection des données par et dès la conception (démarche dite « privacy by design »), qui vise à limiter les risques liés aux traitements de données à caractère personnel via l'adoption de mesures adéquates et proactives.

Les Utilisateurs sont informés que la Charte peut être amenée à évoluer en fonction des différentes évolutions et interprétations du Règlement.

Clé de lecture de la Charte

	Chaque règle énoncée est marquée par ce symbole.
	Chaque bonne pratique (ou recommandation) énoncée est marquée par ce symbole. Elle n'a pas de caractère obligatoire.

SOMMAIRE :

ARTICLE 1 – CHAMP D'APPLICATION DE LA CHARTE

1.1 – Tout Utilisateur doit prendre connaissance de la Charte avant d'avoir accès aux Outils Numériques. A cet effet, tout nouvel arrivant à IXAD se verra communiquer un exemplaire de la Charte via le règlement intérieur, devra en prendre connaissance dans les plus brefs délais et les signer en double exemplaire.

1.2 – La Charte s'applique aux Utilisateurs des Outils Numériques dans le cadre d'activités intervenant sur le réseau et/ou les équipements numériques de IXAD et par conséquent notamment à l'ensemble des salariés de IXAD indépendamment de leur lieu d'activité.

Les Outils Numériques comprennent les équipements informatiques installés, configurés et paramétrés par le personnel habilité par IXAD et mis à disposition dans les locaux de IXAD, et notamment les ordinateurs fixes, les ordinateurs portables, les serveurs, le réseau, les unités de stockage, les clés USB cryptées mises à disposition par IXAD, le matériel de téléphonie, fixe et mobile, etc.

1.3 - Les Outils Numériques sont mis à la disposition des Utilisateurs à des fins professionnelles.

1.4 – Les intervenants extérieurs peuvent bénéficier d'un accès aux Outils Numériques et au réseau de IXAD. Ils sont donc soumis au respect de la Charte, dans les conditions définies ci-après.

ARTICLE 2 – PROTECTION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre de la mise en conformité au regard du droit des données à caractère personnel, cette charte vise également à informer les Utilisateurs des « bonnes pratiques » à accomplir.

L'expression « les bonnes pratiques » désigne un ensemble de règles qui permet de concourir à une utilisation plus sécurisée des Outils Numériques.

2.1 – Les principes encadrant les traitements de données à caractère personnel

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée (ci-après, la « **Loi Informatique et Libertés** ») et le Règlement définissent les conditions selon lesquelles les traitements de données à caractère personnel doivent être effectués :

- Les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (**principe de licéité, de loyauté et de transparence**) ;
- Elles doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (**principe de limitation des finalités**) ;
- Elles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (**principe de minimisation des données**) ;
- Elles doivent être exactes et, si nécessaire, tenues à jour : toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (**principe d'exactitude**) ;

- Elles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées puis, le cas échéant, être archivées pendant une durée limitée dans un espace de stockage distinct avec accès restreint (**principe de limitation de la conservation**) ;

- Elles doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (**principe d'intégrité et de confidentialité**).

2.2 – Engagements des Utilisateurs

Les Utilisateurs s'engagent à respecter les dispositions du Règlement, de la Loi Informatique et Libertés et de tout autre texte relatif à la protection des données à caractère personnel, applicable dans le cadre de leurs activités professionnelles. Ils s'engagent également à respecter les modalités de traitement définies par IXAD, et notamment à :

- Respecter la confidentialité des données à caractère personnel qu'ils traitent pour le compte de IXAD ;

- Privilégier les outils et les logiciels fournis par IXAD pour traiter organiser les données à caractère personnel qu'ils sont amenés à traiter, et limiter leur utilisation de supports alternatifs (clés USB personnelles, tableurs Excel, notes « papier », etc.) ;

- Respecter les durées de conservation des données à caractère personnel définies par IXAD et s'assurer que les documents et les données dont la durée de vie a atteint son terme sont bien détruits ou supprimés ;

- N'utiliser les données à caractère personnel collectées par IXAD que selon ses instructions, et en tout état de cause à ne pas les traiter pour des finalités différentes que celles qui ont été initialement prévues sans accord explicite de IXAD ;

- Faire part de toute suspicion d'intrusion dans les locaux ou dans le système informatique de IXAD à la Direction ; lui faire part plus généralement de toute suspicion d'atteinte à la confidentialité, l'intégrité ou la disponibilité des données.

2.3 – Le registre des traitements

Dans le cadre de la nouvelle règlementation applicable, IXAD doit tenir un document interne retraçant l'ensemble des traitements de données à caractère personnel réalisés au sein de l'organisme.
Si un membre du personnel de IXAD souhaite réaliser un traitement de données à caractère personnel ou faire évoluer les finalités d'un traitement de données à caractère personnel préexistant, celui-ci doit informer préalablement le service juridique de IXAD avant de procéder à la réalisation dudit traitement.

IXAD s'engage à tenir ce registre de traitement et à le mettre régulièrement à jour. A ce titre, ce registre sera complété au fur et à mesure de la mise en œuvre des traitements de données à caractère personnel.

2.4 – Traitement des données relatives aux membres du personnel

Dans le cadre de la mise à disposition aux Utilisateurs des Outils Numériques, IXAD est susceptible de traiter des données à caractère personnel leur étant relatives à des fins de gestion technique, de gestion administrative et de sécurité. Les Utilisateurs bénéficient sur leurs données d'un droit d'accès, de rectification, d'opposition, de limitation, d'effacement et de portabilité, qu'ils peuvent exercer en contactant IXAD à l'adresse suivante, en joignant à leur demande un justificatif d'identité :

IXAD NORD-OUEST
1 Place Déliot
BP629
59024 LILLE CEDEX

Courriel : informatique@ixad.fr

Pour plus d'informations relatives aux traitements qui sont faits de leurs données à caractère personnel, IXAD invite les Utilisateurs à consulter sa politique de protection des données à caractère personnel.

ARTICLE 3 – REGLES D'UTILISATION DES OUTILS NUMERIQUES

Les Outils Numériques sont et demeurent la propriété exclusive de IXAD.

Chaque Utilisateur peut accéder aux Outils Numériques nécessaires à l'exercice de son activité professionnelle à condition de respecter les dispositions de la Charte.

3.1 – Les règles d'utilisation des Outils Numériques

Les Outils Numériques sont mis à la disposition des Utilisateurs à des fins professionnelles.

	L'Utilisateur s'engage à prendre soin des équipements qui lui sont confiés.
	L'Utilisateur s'interdit de modifier les Outils Numériques, leur fonctionnement, et leur configuration logicielle d'une quelconque manière, et notamment par l'installation, la copie, la modification et la suppression de logiciels et/ou de matériel sans en avoir préalablement obtenu l'autorisation écrite de sa hiérarchie.
	L'Utilisateur s'interdit de connecter des équipements non fournis et/ou non autorisés par IXAD sur le réseau interne ou sur un poste de travail.
	L'Utilisateur s'interdit de désactiver les programmes ou services de sécurité installés sur les Outils Numériques.
	En cas d'absence temporaire planifiée, l'Utilisateur s'engage à mettre en place avant son départ les actions appropriées afin d'assurer la continuité et la qualité du service rendu.
	L'Utilisateur s'interdit de mettre en œuvre un accès externe au système d'information de IXAD ou à tout élément d'infrastructure sans l'accord préalable écrit de son supérieur hiérarchique.
	Lorsque l'Utilisateur utilise les logiciels et les bases de données, il s'engage à respecter les dispositions du code de la propriété intellectuelle.

	L'utilisation des Outils Numériques à titre privé est tolérée, à condition qu'il s'agisse d'une utilisation ponctuelle et raisonnable qui ne perturbe pas le bon fonctionnement de l'activité de IXAD ou de son système d'information.
	L'Utilisateur s'engage à ne pas utiliser les Outils Numériques à titre privé à des fins lucratives.
	L'Utilisateur s'engage à ne pas désactiver les Outils et moyens de prise de main à distance de leur poste de travail (utilisés dans le cadre du dépannage de leur poste ou du télétravail par exemple)

3.3 – Degré d'accès aux Outils Numériques

La mise à disposition des Outils Numériques s'effectue en conformité avec le « profil Utilisateur ».

L'accès aux Outils Numériques nécessite l'attribution de droits d'accès spécifiques à chaque profil, qui sont personnels et incessibles, après acceptation de la Charte.

Les droits conférés aux Utilisateurs sont attachés à la fonction exercée au sein de IXAD et peuvent de ce fait être :

- Modifiés en cas de changement de poste ou d'évolution de la fonction exercée ;
- Supprimés automatiquement lorsque l'Utilisateur quitte ou termine sa mission pour IXAD ou s'il est prouvé qu'il y a eu violation de la Charte.

ARTICLE 4 – REGLES DE SECURITE DES OUTILS NUMERIQUES

4.1 – IXAD s'engage à mettre en œuvre les moyens appropriés afin d'assurer la sécurité matérielle et logicielle des Outils Numériques.

4.2 – L'authentification

L'accès aux Outils Numériques repose sur l'utilisation d'un identifiant fourni à l'Utilisateur lors de son arrivée à IXAD. Un mot de passe est ensuite associé à cet identifiant de connexion. L'Utilisateur devra changer ce mot de passe dès sa première connexion, par mesure de sécurité.

L'authentification est une mesure de sécurité importante. Ainsi, chaque Utilisateur doit se conformer aux règles suivantes :

	Les moyens d'authentification sont strictement personnels et confidentiels ;
	Chaque Utilisateur a conscience que la solidité d'un mot de passe dépend de sa complexité. Ainsi, il convient de choisir un mot de passe de qualité, d'une longueur minimale suffisante, répondant aux exigences de complexité du service informatique de IXAD ;
	Chaque mot de passe doit être composé de douze (12) caractères minimums, combinant chiffres, lettres, au moins une majuscule et un caractère spécial ;
	Chaque Utilisateur s'engage à modifier impérativement les mots de passe définis par défaut lorsque les systèmes en contiennent.

4.3 - Pour assurer une sécurité optimale, l'Utilisateur est invité à prendre en considération les bonnes pratiques suivantes :

	Utiliser un mot de passe unique pour chaque service. En particulier, l'utilisation d'un même mot de passe entre la messagerie professionnelle et la messagerie personnelle est impérativement à proscrire ;
	Choisir un mot de passe qui n'a pas de lien avec sa vie personnelle (la date de naissance est par exemple à proscrire, tout comme les prénoms, ou tout autre terme issu du dictionnaire et pouvant être aisément piraté par « force brute ») ;
	Ne pas conserver d'enregistrement sur les informations secrètes d'authentification (par exemple sur support papier, ficher électronique ou équipement portable), sauf si le support de stockage est sécurisé et si la méthode de stockage a été approuvée (par exemple un coffre-fort électronique).

4.5 – Les règles de sécurité

Chaque Utilisateur s'engage à respecter les règles de sécurité suivantes :

	Être vigilant et signaler immédiatement à son supérieur hiérarchique et/ou au service informatique, tout dysfonctionnement, incident et anomalie des Outils Numériques dont il aurait connaissance.
	Signaler au service compétent, toute violation ou tentative de violation suspectée et toute intrusion et faille de sécurité des Outils Numériques.
	Informer sans délai IXAD de toute altération, perte, vol, destruction ou tout autre évènement pouvant affecter les Outils Numériques.
	S'assurer de toujours verrouiller et sécuriser son ordinateur dès son absence sur le poste de travail (touche Windows + L).
	Veiller à n'apporter, directement ou indirectement, aucune perturbation au fonctionnement du réseau et des systèmes informatiques, à ne provoquer aucune modification, altération ou destruction concernant des données ou fichiers autres que ceux dont il est l'auteur ou dont il a la charge, et à ne pas effectuer des opérations pouvant nuire aux relations internes et externes de IXAD.
	Ne jamais pré-enregistrer son identifiant et son mot de passe dans le navigateur ;
	Ne jamais demander ou tenter de connaître l'identifiant et le mot de passe d'un autre Utilisateur.
	Ne pas masquer ou tenter de masquer son identité.
	Ne pas usurper l'identité d'une tierce personne.
	Ne pas installer ou copier de logiciels, de fichiers ou tout autre module susceptibles de générer des risques de sécurité pour le système d'information de IXAD.
	Ne pas copier, modifier ou détruire les logiciels couverts par des droits de propriété intellectuelle.

	Ne pas réaliser de copie de données sur un support externe non sécurisé.
	Effectuer des sauvegardes régulières des fichiers professionnels
	Ne pas utiliser des moyens de cryptographie sans autorisation préalable de son supérieur hiérarchique.
	Respecter les règles de sécurité mises en œuvre par IXAD.

En outre, chaque Utilisateur s'engage à prendre en considération les recommandations suivantes :

	Lorsque les Utilisateurs traitent des données sensibles, ils s'engagent à tout mettre en œuvre pour réduire les risques de sécurité et de divulgation, afin que ces informations ne puissent pas être interceptées par des personnes non autorisées.
	Chaque Utilisateur est invité à supprimer régulièrement les données devenues inutiles sur les espaces communs de stockage de IXAD. Les données à archiver peuvent être conservées avec l'accord de IXAD.

ARTICLE 5 – EQUIPEMENT PERSONNEL NUMERIQUE DES SALARIES DE IXAD : « BRING YOUR OWN DEVICE »

5.1 – L'expression « Bring your own device » peut être traduit en français comme « Apportez votre équipement personnel de communication ».

5.2 – Les salariés de IXAD sont autorisés à apporter leurs appareils numériques personnels sur leur lieu de travail, sous réserve de :

	Chiffrer leur appareil numérique et assurer la sécurité des échanges professionnels ;
	Respecter les règles relatives à la conformité des ordinateurs portables en termes de licences (système d'exploitation et antivirus), de sécurité des données et des accès, énoncées par IXAD ;
	Ne se connecter au réseau professionnel de IXAD avec son smartphone personnel qu'après autorisation expresse de la direction.

5.3 – Tout Utilisateur est invité à réaliser une séparation entre l'utilisation privée et l'utilisation professionnelle des Outils Numériques, afin de protéger les données liées à l'activité de IXAD.

5.4 – IXAD fournit les logiciels nécessaires à l'exercice des fonctions de ses salariés

5.5 – Le personnel de IXAD s'engage à tout mettre en œuvre pour assurer la sécurité de son équipement personnel et ainsi à ne pas porter atteinte, directement ou indirectement, aux Outils Numériques de IXAD.

5.6 – Nonobstant ce qui précède, et conformément aux dispositions du Code du Travail et à la Jurisprudence applicable, IXAD s'engage à respecter la vie privée du salarié.

ARTICLE 6 – MOYENS DE COMMUNICATION A DISTANCE

Les Outils Numériques comprennent les moyens de communication à distance, notamment la téléphonie, la messagerie électronique et l'accès à internet.

6.1 – Téléphonie et accès à distance

Dans le cadre de son activité professionnelle, l'Utilisateur peut disposer de moyens de télécommunication permettant l'échange de données et le transfert de la voix. Ces outils peuvent consister en des équipements terminaux de télécommunication ou de postes de travail permettant de bénéficier d'une téléphonie sous IP (Internet Protocole) ou de tout autre moyen technologique permettant les transmissions de données ou de transfert de voix.

Il est rappelé que l'envoi de sms est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel. Il est donc soumis aux mêmes règles que pour les courriers postaux et les emails.

IXAD met en œuvre un suivi de l'utilisation des moyens de communication. En cas d'utilisation manifestement anormale, IXAD peut avoir accès aux numéros complets des relevés individuels.

Les communications téléphoniques d'ordre personnel ne sont tolérées que dans la mesure où elles ne sont pas pénalisantes pour l'entreprise, en raison notamment de leur fréquence, durée ou coût. L'Utilisateur s'engage à ne pas outrepasser cette tolérance.

6.2 – Internet

La navigation Internet est une ressource informatique mise à la disposition de chaque Utilisateur par IXAD, pour ses besoins professionnels. L'Utilisateur s'engage à en faire un usage respectueux de la Charte, de la loi et de l'ordre public.

Il est précisé à chaque Utilisateur que la libre accessibilité aux informations, contenues dans les sites web auxquels il accède, n'inclut pas nécessairement la libre réutilisation de ces informations dans le cadre d'une activité professionnelle. A ce titre, l'Utilisateur veillera à respecter les dispositions du code de la propriété intellectuelle.

6.3 – Messagerie électronique

6.3.1 - Conditions d'utilisation :

Chaque Utilisateur se voit attribuer un compte de messagerie et un accès au portail de IXAD.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par IXAD.

Le compte de messagerie mis à la disposition des Utilisateurs est destiné à un usage strictement professionnel.

L'utilisation de l'adresse de messagerie professionnelle dans le cadre d'activités personnelles est à limiter au maximum. En effet, les Utilisateurs sont invités à utiliser leur messagerie personnelle pour l'envoi de messages à caractère personnel plutôt que leur messagerie professionnelle.

IXAD rappelle qu'un message électronique a la même portée qu'un courrier postal et obéit donc aux mêmes règles, en particulier en termes d'organisation hiérarchique et de secret des correspondances.

A des fins de sécurité, une attention particulière doit être portée à l'ouverture des pièces jointes des emails, afin de prémunir IXAD contre tout risque de virus (malware etc.). En cas de message ou de pièce jointe douteux, il est recommandé de ne pas ouvrir l'email ou la pièce jointe et de prévenir sans délai la direction de IXAD.

L'accès à la messagerie est un droit personnel, nominatif et incessible. Le possesseur de droit d'accès est responsable de la confidentialité des codes d'accès à son poste de travail.

Il en résulte que si l'Utilisateur communique son identifiant et/ou son mot de passe à une tierce personne, celui-ci s'engage à endosser la responsabilité de toutes les infractions qui pourraient être commises par la personne qui utilise cet identifiant et/ou ce mot de passe.

Tout message qui comporte la mention expresse ou manifeste de son caractère personnel (**avec la mention « personnel »)** bénéficie du droit au respect de la vie privée et du secret des correspondances. Il appartient à l'Utilisateur de procéder au stockage de ses messages personnels dans un répertoire spécialement créé à cet effet, intitulé « personnel », de manière raisonnable, aux espaces alloués. A défaut, le message est présumé être professionnel.

IXAD s'interdit d'accéder aux dossiers et aux messages identifiés comme personnels, sauf accord de l'Utilisateur et en sa présence.

6.3.2 - Consultation de la messagerie :

	En cas d'absence supérieure à un (1) jour, les Utilisateurs s'engagent à mettre en place une réponse automatique aux emails, afin d'informer les interlocuteurs de leur absence et de leur date de disponibilité ;
	En cas d'absence prolongée, l'Utilisateur concerné doit mettre en place un relai pour ses emails professionnels vers un salarié de IXAD, afin que son absence ne puisse pas avoir d'incidence sur le fonctionnement de l'activité de la société.

ARTICLE 7 – ACCES A DISTANCE ET EQUIPEMENTS NOMADES

Les Outils Numériques comprennent les moyens d'accès à distance, notamment par des équipements nomades. Les équipements nomades sont l'ensemble des matériels électroniques pouvant être transportés hors du lieu de travail effectif (par exemple, un ordinateur portable, une clé USB, un téléphone portable…)

7.1 – Partage de données accessibles à distance

Dans le cadre du partage de données effectué pour un usage professionnel, conformément aux politiques de sécurité, IXAD invite les salariés à privilégier le partage de données via les fonctionnalités offertes par le système d'information et à prendre toute précaution utile pour sécuriser les supports USB ainsi que les données qui y sont stockées.

Les Utilisateurs sont autorisés à réaliser du partage de fichiers en ligne pour des données ne présentant pas un risque pour leur sécurité ou leur divulgation. Toutefois, cette pratique doit être limitée pour les données sensibles.

7.2 – Télétravail

Pour le personnel de IXAD habilité à travailler en dehors de l'enceinte des locaux, les Outils Numériques sont mis à leur disposition selon les modalités prévues à cet effet. Leur usage est à privilégier par rapport aux équipements personnels.

L'Utilisateur s'engage à appliquer des mesures de sécurité aux Outils Numériques utilisés hors des locaux de IXAD en tenant compte des différents risques associés au travail hors site.

L'Utilisateur reconnaît avoir pleinement conscience des conséquences préjudiciables à IXAD qui pourraient résulter de la perte des équipements nomades, de leur soustraction frauduleuse par autrui ou de l'accès par un tiers à leur contenu (par exemple la perte financière, la perte ou fuite d'informations ou de données présentant un caractère confidentiel etc.).

Dans ce cadre, l'Utilisateur s'engage à :

	Utiliser les équipements nomades mis à sa disposition ;
	Ne pas laisser les équipements nomades sans surveillance ;
	Respecter les consignes relatives à la mise en œuvre de la connexion ;
	Assurer la garde des équipements nomades mis à sa disposition ;
	Ne jamais pré-enregistrer son identifiant et son mot de passe dans le navigateur ;
	Informer immédiatement la direction de IXAD en cas d'incident relatif aux équipements nomades et à assister IXAD ou à procéder lui-même à toutes les démarches rendues nécessaires à la suite d'un incident de quelque nature que ce soit ;
	Mettre en œuvre des mesures de sécurité pour protéger les informations consultées, traitées ou stockées sur les sites de télétravail ;

7.3 - Il convient pour l'utilisateur de :

	Ne pas laisser les équipements nomades sans surveillance à l'intérieur et l'extérieur des bâtiments de IXAD.
	Veiller à la bonne réalisation de ses sauvegardes en utilisant les procédures et les outils mis à sa disposition.

7.4 – En toute hypothèse, l'Utilisateur, qui est responsable des équipements nomades mis à sa disposition, en assure la garde.

	En cas d'incidents tels que le vol, la perte ou la dégradation du matériel, l'Utilisateur doit en informer IXAD dans les plus brefs délais afin qu'il soit procédé aux démarches nécessaires.
	L'Utilisateur assiste IXAD ou procède lui-même, selon les cas, à toutes les démarches (déclaration d'assurance, plainte etc.) rendues nécessaires.

ARTICLE 8 – ADMINISTRATION DU SYSTEME D'INFORMATION DE IXAD

Afin de surveiller le fonctionnement et de garantir la sécurité des Outils Numériques de IXAD, plusieurs mesures ont été mises en place.

8.1 – Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités et du blocage de certains protocoles (exemple : le « peer to peer »).

8.2 – Gestion du poste de travail

A des fins de maintenance ou d'assistance informatique, l'Utilisateur peut être invité à donner accès à ses Outils Numériques pour des interventions à distance réalisées par des prestataires autorisés par IXAD.

Dans le cadre d'opérations de maintenance, de mises à jour et d'évolutions du système d'information, IXAD peut demander à un prestataire d'accéder à distance à l'ensemble des postes de travail du personnel.

Le prestataire ne vous demandera en aucun cas de lui fournir votre mot de passe, et utilisera pour ses opérations de maintenance un logiciel d'accès à distance.

8.3 – Mesures de contrôle et de surveillance

IXAD peut procéder à des traitements de données afin de surveiller l'activité du système d'information :

- A l'utilisation des logiciels applicatifs ;
- Au contrôle d'accès ;
- Aux sites consultés par l'utilisateur
- Aux créations, modifications, suppressions de fichiers ou de données.

Les Utilisateurs sont informés que IXAD peut mettre en œuvre toutes opérations techniques de contrôle permettant de vérifier le respect des dispositions de la Charte ou des règles légales.

Dans le cadre d'une opération de contrôle concernant spécifiquement un Utilisateur, le contrôle sera mené par des personnes dûment habilitées qui pourront notamment ouvrir sans l'accord de l'Utilisateur, les fichiers et messages non classifiés « personnel » ou « privé », conformément aux règles légales applicables en vigueur.

ARTICLE 9 – CONFIDENTIALITE ET DEVOIR DE RESERVE

9.1 – Utilisation des réseaux sociaux

Les Utilisateurs sont soumis à un devoir de loyauté et de réserve, tant dans un usage professionnel que personnel des réseaux sociaux.

La liberté d'expression est soumise au devoir de réserve. Ainsi, l'Utilisateur s'engage à ne pas émettre d'opinions personnelles susceptibles de porter préjudice à IXAD.

De manière générale, les Utilisateurs s'engagent à signaler tout commentaire de tiers concernant IXAD qui semblerait abusif et/ou qui porterait atteinte aux droits de IXAD, et a fortiori qui porterait atteinte à l'image de IXAD.

Les Utilisateurs ne doivent pas s'exprimer au nom de IXAD sans y avoir été dûment habilités.

Les Utilisateurs doivent veiller à ne communiquer ou diffuser aucune information de IXAD sur les réseaux sociaux, notamment des informations confidentielles et/ou sensibles.

9.3 – Confidentialité des informations propres à IXAD

Les Utilisateurs s'engagent à ne pas communiquer à des tierces personnes tout document appartenant à ou confié à IXAD ou plus généralement tout document confidentiel. En cas de non-respect de cette obligation de confidentialité, l'Utilisateur s'expose à des sanctions disciplinaires et/ou civiles.

Compte tenu de la possibilité d'accéder à distance aux Outils Numériques de IXAD, les Utilisateurs s'engagent à tout mettre en œuvre pour protéger la sécurité et la confidentialité du patrimoine informationnel de IXAD.

A ce titre, les Utilisateurs assument l'entière responsabilité de leur négligence en cas d'atteinte au patrimoine informationnel de IXAD.

9.4 – Comportements interdits

L'Utilisateur s'engage à respecter les règles suivantes :

Il est interdit de consulter, charger, stocker, publier ou distribuer, au moyen des ressources de IXAD, des documents, informations, images, vidéos ou tout autre média :

- A caractère violent, pornographique, pédophile, raciste, contraires aux bonnes mœurs, ou susceptibles de porter atteinte au respect de la personne humaine et à sa dignité ;
- En violation de la loi ;
- A caractère diffamatoire, et de manière générale illicite ;
- Utilisés à des fins de harcèlement, menace ou injure ;
- Dans le but de procéder à des envois massifs ou en chaîne de courriers électroniques non sollicités ;
- Dans le but de porter atteinte à l'intégrité, au bon fonctionnement, à la propriété intellectuelle, aux intérêts et à l'image, à la réputation de IXAD ou de tiers ;
- Dans le but de porter ou susceptible de porter atteinte aux secrets d'affaires de IXAD, de ses partenaires ou de ses clients.

Dans le cas où un Utilisateur recevrait à son insu de tels documents, il doit en informer dans les plus brefs délais la direction de IXAD. Des sanctions pénales peuvent dans certains cas être applicables aux Utilisateurs se rendant coupables de violation de la loi dans l'usage des Outils Numériques.

En cas de procédure judiciaire pour une infraction présumée aux dispositions énoncées ci-dessus, IXAD pourrait être tenue de communiquer à l'autorité judiciaire l'ensemble des éléments d'information qui lui seraient demandés.

ARTICLE 10 – SAUVEGARDE DES DONNEES ET MAINTENANCE

10.1 – L'Utilisateur a la responsabilité de procéder à la sauvegarde régulière des données professionnelles qui se trouvent sur son poste de travail dans le respect des procédures en vigueur et ce, pour des raisons de sécurité telles qu'énoncées dans la Charte.

10.2 – La mise à disposition d'Outils Numériques implique nécessairement des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, préventive ou évolutive.

L'objectif de ces opérations est d'assurer le bon fonctionnement et la sécurité des systèmes d'informations.

L'Utilisateur devra se conformer aux différentes demandes de maintenance sur son poste de travail et sera tenu de les accepter, notamment concernant les demandes de maintenance automatique. Il pourra planifier ces mises à jour automatiques en respectant les délais mentionnés et ne devra pas s'opposer au bon déroulement de ces mises à jour.

Dans le cas où ces opérations de maintenance nécessitent une intervention sur site ou une « prise en main à distance », ces opérations seront exclusivement réalisées par une personne habilitée, désignée à cet effet par IXAD. Celle-ci est tenue de respecter la confidentialité des informations auxquelles elle accède dans le cadre de sa mission.

10.3 – Conformément aux règles légales applicables, l'accès aux répertoires intitulés « personnel » ou « privé » se fait uniquement en présence de l'Utilisateur, après l'avoir invité à être présent, ou en cas de risque particulier pour IXAD.

Dans ce dernier cas, la personne habilitée désignée par IXAD peut être amenée, pour des raisons de sécurité ou techniques présentant un risque particulier pour l'école, et ce, malgré l'opposition ou l'absence de l'Utilisateur, à accéder auxdits répertoires.

ARTICLE 11 – PROCEDURE APPLICABLE LORS DU DEPART D'UN UTILISATEUR

11.1 – En cas de départ d'un Utilisateur pour quelque cause que ce soit, celui-ci doit restituer à IXAD le matériel et les documents professionnels mis à sa disposition dans le cadre de son activité professionnelle.

La non-restitution du matériel et des documents appartenant à IXAD est passible de poursuite judiciaire.

11.2 – Au préalable, celui-ci devra effacer tout fichier et données à caractère privé qui serait stocké sur les Outils Numériques.

11.3 – Toute copie de documents et fichiers professionnels est strictement interdite.

11.4 – IXAD demandera au service de gestion des accès la désactivation du compte et la suppression des droits d'accès de l'Utilisateur concerné.

En toute état de cause, le compte ainsi que les données à caractère personnel de l'Utilisateur seront supprimés définitivement dans un délai maximum de douze (12) mois après son départ.

ARTICLE 12 – RESPONSABILITES ET SANCTIONS

12.1 – Le manquement aux règles et aux mesures de sécurité et de confidentialité définies par la Charte est susceptible d'engager la responsabilité de l'Utilisateur et d'entrainer des sanctions disciplinaires à son encontre.

12.2 – En sus de ces sanctions disciplinaires, l'Utilisateur est conscient que s'il ne respecte pas le droit applicable constitué notamment par la Loi Informatique et Liberté et le RGPD, il est susceptible d'encourir le prononcé de sanctions civiles et pénales.

ARTICLE 13 – ENTREE EN VIGUEUR DE LA CHARTE

La Charte est applicable à partir du 1er Juin 2020

ARTICLE 14 – FORMALITES

Chaque Utilisateur s'engage à prendre connaissance et à observer l'ensemble des dispositions de la Charte.

Conformément au Code du travail, la Charte fera l'objet d'une communication et d'un dépôt auprès :

- De l'inspection du travail ;
- Du personnel de IXAD ;

Fait en double exemplaire à LILLE,

Le 1er Juin 2020.

Signature de l'Utilisateur,

Précédée de la mention « lu et approuvé »