

Charte d'utilisation des moyens Informatiques pour les élèves du Lycée Jean Mermoz

La charte informatique a pour objectif d'informer les élèves des règles qui s'imposent quant à l'utilisation d'un système d'information et l'exploitation de ses ressources. Elle permet aussi de fixer de manière transparente les conditions dans lesquelles la responsabilité des élèves peut être mise en cause.

Préambule	3
Droits et devoirs	3
Droits	3
Devoirs	3
Champ d'application	4
Utilisateurs concernés	4
Système d'information et de communication	4
Confidentialité	4
Paramètres d'accès	4
Données	5
Besoins auxquels répond le système d'information	5
Sécurité	5
Rôle de l'Établissement	5
Responsabilité de l'élève	6
Quelques bonnes pratiques à respecter	6
Internet	6
Accès aux sites	6
Autres utilisations	7
Messagerie électronique	7
Conseils généraux	7
Limites techniques	7
Utilisation personnelle de la messagerie	8
Contrôle des activités	8
Contrôles automatisés	8
Information et sanctions	8
Entrée en vigueur	9
Protection des données personnelles et sécurité	9
Acteurs et responsables	9
Annexe	10
Liens utiles	10
Glossaire	11

Préambule

Le Lycée franco-argentin Jean Mermoz met à disposition de ses élèves un système d'information (SI) et des moyens informatiques nécessaires à son activité, comprenant notamment un réseau informatique ainsi que des outils mobiles.

L'utilisation du système d'information et de communication se fait exclusivement à des fins pédagogiques.

Dans un but de transparence à l'égard des élèves, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et de communication, la présente charte pose les règles relatives à l'utilisation de ces ressources.

Cette charte a pour objectif :

- De sensibiliser les élèves aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu'ils sont amenés à effectuer ;
- D'informer les élèves sur :
 - Les usages permis des moyens informatiques mis à sa disposition ;
 - Les règles de sécurité en vigueur ;
 - Les mesures de contrôle prises par l'établissement ;
- De formaliser les règles générales de sécurité que les élèves s'engagent à respecter, en contrepartie de la mise à disposition des systèmes d'information et des équipements informatiques, et ainsi de déterminer les droits et devoirs des élèves.

Droits et devoirs

Droits

Les élèves ont le droit :

- d'accéder aux ressources numériques mises à disposition par l'établissement (ordinateurs, tablettes, logiciels pédagogiques, internet...).
- d'utiliser les services en ligne de l'école (messagerie, espace de travail, plateformes éducatives) dans le cadre des activités pédagogiques.
- d'être accompagnés et formés à un usage responsable et sécurisé du numérique.
- Voir leur vie privée respectée, notamment en ce qui concerne leurs données personnelles et la confidentialité de leurs travaux scolaires.
- de travailler dans un environnement numérique sécurisé, protégé des contenus inappropriés et des cybermenaces.
- d'exprimer des besoins ou signaler des incidents (matériel défectueux, cyberharcèlement, difficultés d'accès, etc.).
- d'accéder à leurs productions numériques et de conserver leurs travaux scolaires.

Devoirs

Les élèves s'engagent à :

1. Utiliser les outils numériques uniquement à des fins scolaires, dans le respect du cadre défini par les enseignants et l'établissement.
2. Protéger leurs identifiants et mots de passe : ne pas les partager, ne pas usurper l'identité d'autrui.
3. Respecter les règles de sécurité informatique (ne pas contourner les filtres, ne pas installer de logiciels non autorisés, ne pas modifier les configurations).
4. Adopter un comportement responsable en ligne : respect d'autrui, politesse, absence de harcèlement ou de propos discriminatoires.
5. Respecter la loi sur les droits d'auteur : ne pas copier, pirater, diffuser du contenu protégé.
6. Ne pas accéder, transmettre ou stocker de contenus choquants, illégaux ou inappropriés.
7. Respecter l'intégrité du matériel informatique : utiliser le matériel avec soin, signaler toute panne ou incident.
8. Ne pas réaliser de photos, de vidéos ou d'enregistrements sans autorisation des personnes concernées et de l'établissement.
9. Signaler immédiatement toute situation mettant en danger la sécurité numérique ou l'intégrité des données.

Champ d'application

Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des élèves utilisateurs du système d'information et de communication du Lycée Jean Mermoz

Système d'information et de communication

Le système d'information et de communication du Lycée Jean Mermoz est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques y compris clés USB, réseau informatique (serveurs, routeurs et connectique), photocopieurs, télécopieurs, tablettes, logiciels, fichiers, données et bases de données, système de messagerie, connexion internet, intranet, extranet.

Confidentialité

Paramètres d'accès

L'accès à certains éléments du système d'information (comme la messagerie électronique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe).

L'utilisation des systèmes informatiques a pour objet exclusif de mener à bien des activités d'enseignement et de documentation.

Chaque élève se voit attribuer un identifiant et un mot de passe qui lui permettent d' :

- Accéder aux ressources informatiques et pédagogiques mise à disposition par l'établissement.
- Accéder aux informations et ressources présentes sur Internet.

Cet identifiant et ce mot de passe sont strictement personnels et confidentiels.

L'établissement met également à disposition des élèves des logins dits « génériques » permettant l'utilisation des salles pédagogiques. Dans le cadre de son activité, l'élève qui utilise un poste informatique reste responsable de l'usage qu'il fait du matériel même s'il ne dispose pas d'un login nominatif et personnel. L'identification éventuelle pouvant être effectuée aux moyens des historiques des événements de l'ordinateur par exemple. De plus l'élève qui se connecte via un compte générique doit s'assurer qu'il ne laisse pas d'informations personnelles sur le poste (fichiers ou sessions personnelles ouverts ...).

Données

L'élève reste vigilant quant au risque de divulgation d'informations personnelles ou appartenant à l'établissement lorsqu'il utilise des outils informatiques.

Aucune donnée confidentielle (documents internes, identifiants, informations sur les élèves ou le personnel) ne peut être partagée avec des personnes ou services non autorisés.

La collecte, la copie ou la diffusion de données issues du système d'information s'effectue uniquement dans un cadre pédagogique validé par l'équipe éducative.

Le droit à l'image s'applique pleinement : aucune photo, vidéo ou enregistrement d'une personne présente dans l'établissement ne peut être publié ou transmis sans son autorisation et celle de l'école.

Besoins auxquels répond le système d'information

Élèves

Les élèves ont accès aux postes de travail de l'établissement situés en salle informatique, au CDI et dans les salles équipées. Ces postes sont équipés d'un antivirus et, d'une suite bureautique.

L'identification se fait au moyen d'un compte générique, commun à plusieurs utilisateurs : les élèves ne doivent donc y enregistrer aucune donnée personnelle et doivent veiller à fermer leurs documents et leur session à la fin de chaque utilisation. L'utilisation des postes se fait sous la responsabilité d'un adulte (enseignant, professeur documentaliste ou assistant d'éducation) et doit répondre à un objectif pédagogique ou scolaire. L'impression est possible sur autorisation de l'adulte responsable. L'accès à Pronote est disponible depuis tout appareil, y compris personnel, depuis l'intérieur comme l'extérieur de l'établissement, afin de consulter l'emploi du temps, le cahier de textes, les notes et d'échanger avec l'équipe éducative via la messagerie intégrée. Enfin, l'accès à Internet depuis l'établissement est filtré afin de protéger les élèves des contenus inappropriés.

Sécurité

Rôle de l'Établissement

L'établissement met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. À ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquiescer les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des élèves.

Le service informatique veille à l'application des règles de la présente charte. Il est assujéti à une obligation de confidentialité sur les informations qu'il est amené à connaître.

Responsabilité de l'élève

L'élève est responsable quant à lui des ressources qui lui sont confiées. Il concourt à la protection des dites ressources, en faisant preuve de prudence et de vigilance. En particulier, il signale au professeur en charge de la classe de toute violation ou tentative de violation de l'intégrité de ces ressources, et, de manière générale, tout dysfonctionnement, incident ou anomalie.

L'élève ne quitte pas son poste de travail et les postes en libre-service dont il a la responsabilité sans fermer la session, laissant ainsi des ressources ou services accessibles des supports informatiques (clé USB, CD-Rom...) contenant des données personnelles accessibles à quelqu'un d'autre.

L'élève n'installe pas ou ne supprime pas des logiciels, ne copie ni n'installe de fichiers susceptibles de créer des risques de sécurité au sein de l'établissement. Il n'est pas autorisé à modifier les paramètres de son poste de travail ou des différents outils mis à sa disposition, ni à contourner aucun des systèmes de sécurité mis en œuvre à l'établissement

Si un élève constate un dysfonctionnement, il alerte le professeur en charge à ce moment-là.

L'élève ne se connecte pas ou n'essaie pas de se connecter sur un site sans y être autorisé ou sur un site sans rapport avec la recherche demandée par le professeur

L'élève s'oblige en toutes circonstances à se conformer à la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes.

Quelques bonnes pratiques à respecter

- Toujours verrouiller son poste lorsque l'on ne l'utilise pas.
- Ne jamais confier son mot de passe d'identification à autrui
- Laisser des informations personnelles sur les postes est fortement déconseillé, d'autant plus si l'utilisateur est connecté sur un compte générique.
- Utiliser des supports amovibles (clef USB, disque dur USB...) est fortement déconseillé.
- Prêter attention aux mails reçus, ne pas cliquer sur un lien sans être sûr que l'expéditeur est une personne de confiance.

Internet

Accès aux sites

Un accès à Internet est attribué aux élèves afin de permettre la consultation des sites web. L'établissement met en œuvre des systèmes de filtrage afin d'interdire l'accès à certains sites dont le contenu lui semble illicite, en contradiction ou sans rapport avec ses objectifs éducatifs, ou requiert l'âge de la majorité. Ce filtrage est

régulièrement mis à jour par l'établissement. Il peut toutefois y avoir un délai pour la détection et le blocage de nouveaux sites.

Autres utilisations

La contribution des élèves à des forums de discussion, systèmes de discussion instantanée, chats, blogs n'est autorisée dans l'établissement qu'à titre pédagogique.

De même, tout téléchargement de fichier, en particulier de fichier média, est prohibé, sauf pour une utilisation pédagogique indiquée par le professeur.

Il est rappelé que les élèves ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte à l'image de l'établissement.

Ils sont informés que le service informatique enregistre leur activité sur Internet et que ces traces pourront être exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi, en particulier en cas de perte importante de bande passante sur le réseau de l'établissement.

Messagerie électronique

La messagerie électronique attribuée par l'établissement à l'élève doit être utilisée exclusivement dans le cadre d'une activité pédagogique.

Les messages électroniques reçus sur la messagerie font l'objet d'un contrôle antiviral et d'un filtrage anti-spam.

Conseils généraux

Un message électronique peut être communiqué très rapidement à des tiers et il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités.

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

Les élèves veillent au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne comportent pas d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants.

Limites techniques

Le service informatique peut limiter la taille, le nombre et le type des pièces jointes pour éviter l'engorgement du système de messagerie. L'élève est tenu de supprimer lui-même dès que possible tous les messages inutiles.

Si l'élève quitte l'établissement (fin de cursus, départ dans un autre établissement...) la messagerie électronique sera suspendu au bout de 3 mois. Et au bout de 6 mois le compte sera supprimé de façon définitive.

Compte suspendu : Il sera possible de récupérer les informations en contactant le service informatique.

Compte supprimé : Le mail n'existe plus et les données liées au mail (Drive Sheet Doc etc....) sont effacés de façon définitive sans possibilité de récupération

Utilisation personnelle de la messagerie

Les élèves sont invités, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'établissement.

Contrôle des activités

Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'établissement, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des élèves accédant au système d'information.

Les élèves sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;
- aux connexions entrantes et sortantes au réseau interne et à Internet, pour détecter les tentatives d'intrusion et les activités, telles que la consultation de sites ou le téléchargement de fichiers.

Dans le cadre de la maintenance informatique mais aussi d'activités pédagogiques ponctuelles, un logiciel de gestion et d'administration des ordinateurs permet la connexion à tout ordinateur identifié sur le réseau de l'établissement ainsi qu'une éventuelle prise en main à distance.

Information et sanctions

La présente charte est affichée publiquement en annexe du règlement intérieur. Chaque élève se conforme aux procédures et règles de sécurité édictées par le service informatique dans le cadre de la présente charte.

Sanctions :

Si les règles de la présente charte ne sont pas respectées, des sanctions seront appliquées en fonction de la gravité des faits :

- Les comptes pourront être suspendus sur décision de la direction
- L'établissement s'autorise à contrôler le contenu des échanges pouvant être faits par les moyens de communication de l'école en cas de signalement
- Des sanctions additionnelles seront appliquées proportionnellement à la gravité du non-respect de la présente charte

Entrée en vigueur

La présente charte est applicable à compter du 01/03/2026

Elle a été adoptée après information et consultation du conseil d'établissement en date du 19 novembre 2025

La présente charte fait l'objet d'une révision au moins tous les trois ans, ou dès lors qu'une évolution majeure du système d'information ou des outils le justifie. À chaque mise à jour, un récapitulatif des modifications sera diffusé à l'ensemble des utilisateurs via le site internet et par messagerie interne.

Protection des données personnelles et sécurité

Le Lycée Jean Mermoz s'engage à traiter les données personnelles de ses utilisateurs dans le respect du Règlement Général sur la Protection des Données (RGPD) et des législations applicables en matière de protection de la vie privée. À ce titre, une politique générale de protection des données, définie sous l'autorité de la direction, encadre l'ensemble des traitements réalisés au sein de l'établissement.

Conformément à l'article 30 du RGPD, tous les traitements de données mis en œuvre dans le cadre du contrôle et de la surveillance du système d'information font l'objet d'un enregistrement dans le registre des activités de traitement de l'établissement, tenu à jour par le Référent RGPD et consultable sur demande auprès de ce dernier.

Les utilisateurs disposent, concernant leurs données personnelles, d'un ensemble de droits qu'ils peuvent exercer à tout moment : droit d'accès, droit de rectification, droit à l'effacement, droit à la limitation du traitement, droit d'opposition. Ces droits s'exercent auprès du Référent RGPD de l'établissement.

Les règles de sécurité informatique appliquées au sein de l'établissement s'appuient sur les référentiels reconnus en la matière, notamment le Guide d'hygiène informatique et le Guide des bonnes pratiques de l'informatique publiés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Un focus sécurité détaillé est mis à disposition des utilisateurs (voir Annexe – Sécurité informatique).

Acteurs et responsables

La direction est responsable de l'application générale de la présente charte. Elle valide les décisions de suspension ou de restriction d'accès au système d'information et arbitre en cas de manquement grave aux règles définies ci-présentes. Au lycée Jean Mermoz, elle est personnifiée par la proviseure :

Françoise STURBAUT
provi@mermoz.edu.ar

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) est chargé de définir et de mettre en œuvre la politique de sécurité informatique de l'établissement. Il identifie les risques, supervise les mesures de protection et veille à leur application.

Cyrille CHAPUIS
cyrille.chapuis@mermoz.edu.ar

Le Référent RGPD est le référent de l'établissement en matière de protection des données personnelles. Il veille au respect du RGPD et des législations applicables, conseille l'établissement sur ses obligations et constitue le point de contact privilégié des utilisateurs pour toute question relative à leurs données personnelles.

Barbara SIMONELLI

barbara.simoncelli@mermoz.edu.ar

Les Référents informatiques assurent au quotidien la gestion technique et la maintenance du système d'information. Ils sont les interlocuteurs directs des utilisateurs pour toute demande d'assistance, signalement d'incident ou attribution de droits d'accès.

Cyrille CHAPUIS

cyrille.chapuis@mermoz.edu.ar

Marcelo PEREZ

marcelo.perez@mermoz.edu.ar

Les Référents sécurité veillent à l'application opérationnelle des règles de sécurité définies par le RSSI. Ils assurent une veille sur les menaces et incidents de sécurité et coordonne les actions correctives en cas d'incident.

Cyrille CHAPUIS

cyrille.chapuis@mermoz.edu.ar

Marcelo PEREZ

marcelo.perez@mermoz.edu.ar

La Direction Administrative et Financière (DAF) veille à la bonne gestion des ressources allouées au système d'information, notamment en matière d'acquisition de matériel, de licences logicielles et de contrats de prestation informatique.

Peggy LEHMANN

peggy.lehmann@mermoz.edu.ar

L'équipe pédagogique et TICE accompagne les apprenants dans leur usage responsable et sécurisé des outils numériques, conformément aux dispositions de la présente charte.

Sebastian BARRASA (Primaire)

sebastian.barrasa@mermoz.edu.ar

Sébastien GRENIER (Secondaire)

sebastien.grenier@mermoz.edu.ar

Annexe

Liens utiles

- Règlement Général sur la Protection des Données (RGPD) – Règlement UE 2016/679 : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679>
- Article 30 du RGPD – Registre des activités de traitement : <https://www.cnil.fr/fr/ce-que-le-rgpd-change-pour-les-responsables-de-traitement>

- Droits des personnes – CNIL : <https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles>
- Guide d'hygiène informatique – ANSSI : <https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique>

L'établissement met à disposition les documents suivants :

- Guide de bon usage informatique : <https://lyceemermoz.edu.ar/v5/wp-content/uploads/Guide-de-bon-usage-doutils-informatiques-Lyce-Franco-Argentin-Jean-Mermoz-2026.pdf>
- Charte de bon usage de l'IA : <https://lyceemermoz.edu.ar/v5/wp-content/uploads/Charte-de-bon-usage-de-lIA-Lyce-Franco-Argentin-Jean-Mermoz-2026-1.pdf>

Glossaire

Administrateur : Membre du service informatique disposant de droits d'accès étendus au système d'information de l'établissement, lui permettant d'en assurer la gestion technique, la configuration, la maintenance et la sécurité. En raison du niveau de privilèges dont il dispose, l'administrateur est soumis à une obligation de confidentialité renforcée et s'engage à n'utiliser ses droits d'accès qu'à des fins strictement professionnelles et dans le respect de la présente charte.

Adresse de messagerie normalisée : Adresse électronique attribuée par le service informatique à chaque membre du personnel, selon un format standardisé défini par l'établissement (ex. : prenom.nom@mermoz.edu.ar). Elle constitue l'adresse officielle à utiliser dans le cadre des échanges professionnels.

Compte utilisateur : Espace d'accès individualisé au système d'information, créé et géré par le service informatique, regroupant les droits, permissions et ressources attribués à un utilisateur donné. Il est strictement personnel et ne peut être utilisé par une autre personne que son titulaire.

Contrôle antiviral / filtrage anti-spam : Le contrôle antiviral désigne le mécanisme automatique d'analyse des messages entrants et sortants visant à détecter et neutraliser les programmes malveillants. Le filtrage anti-spam désigne quant à lui le dispositif de détection et de blocage des messages non sollicités ou indésirables.

Copie cachée (Cci) : Fonctionnalité de la messagerie électronique permettant d'adresser un message à un ou plusieurs destinataires sans que leur identité et leur adresse électronique ne soient visibles des autres destinataires. Son utilisation est recommandée lors d'envois groupés afin de protéger les données personnelles des destinataires.

Fichiers journaux (« logs ») : Enregistrements automatiques générés par les équipements informatiques et de télécommunication, qui tracent l'ensemble des événements et activités survenant sur le système d'information (connexions, accès aux fichiers, erreurs, etc.). Ils constituent un outil essentiel pour la sécurité, la maintenance et le contrôle des usages.

Filtrage / mécanismes de filtrage : Ensemble de dispositifs techniques mis en place par le service informatique permettant de contrôler et de restreindre les flux d'informations entrant et sortant du système d'information. Ils s'appliquent notamment à la navigation Internet, aux messageries électroniques et aux accès réseau, afin de bloquer les contenus inappropriés, malveillants ou non conformes à la politique de l'établissement.

Intervenant extérieur / prestataire : Toute personne physique ou morale extérieure à l'établissement amenée à utiliser, de manière ponctuelle ou régulière, tout ou partie du système d'information dans le cadre d'une mission ou d'une prestation de service. Son accès aux ressources informatiques est conditionné à la signature de la présente charte et limité aux seules ressources nécessaires à l'accomplissement de sa mission.

Intranet / Extranet : L'intranet désigne le réseau interne de l'établissement, accessible uniquement à ses utilisateurs autorisés. L'extranet en est le prolongement sécurisé, permettant à des partenaires ou prestataires extérieurs d'accéder à une partie limitée et définie des ressources de l'établissement.

Liste de diffusion : Adresse électronique unique permettant d'adresser simultanément un message à un groupe d'utilisateurs prédéfinis. La création et la gestion des listes de diffusion relèvent exclusivement du service informatique.

Login nominatif / login générique : Le login nominatif est un identifiant de connexion attribué personnellement à un utilisateur identifié, lui permettant d'accéder au système d'information sous sa propre responsabilité. Le login générique est un identifiant partagé, non rattaché à une personne en particulier, destiné à un usage ponctuel ou collectif (salles pédagogiques, postes en libre-service). Son utilisation n'exonère pas l'utilisateur de sa responsabilité.

Messagerie électronique : Service de communication numérique permettant l'envoi et la réception de messages électroniques entre utilisateurs, via le réseau informatique de l'établissement ou Internet. Son usage dans le cadre professionnel est soumis aux règles définies par la présente charte.

Paramètres de connexion (identifiant, mot de passe) : Couple d'informations personnelles et confidentielles permettant à un utilisateur de s'authentifier sur le système d'information. L'identifiant permet de reconnaître l'utilisateur, tandis que le mot de passe, connu de lui seul, garantit que l'accès ne peut être effectué que par lui. Ces paramètres ne doivent en aucun cas être communiqués à un tiers.

Phishing (hameçonnage) : Technique de fraude informatique consistant à usurper l'identité d'un organisme de confiance (banque, administration, établissement scolaire, etc.) afin de tromper l'utilisateur et de l'inciter à divulguer des informations confidentielles telles que ses identifiants de connexion ou ses coordonnées bancaires. Il se manifeste généralement par l'envoi de messages électroniques frauduleux ou par la création de sites web imitant des sites légitimes.

Pièces jointes : Fichiers de tout format (documents, images, vidéos, etc.) annexés à un message électronique. Leur taille, leur nombre et leur type peuvent être limités par le service informatique pour des raisons de sécurité et de performance du système de messagerie.

Prise en main à distance : Fonctionnalité technique permettant au service informatique d'accéder à un poste de travail connecté au réseau de l'établissement, à des fins de maintenance, d'assistance ou de contrôle, sans nécessiter une intervention physique sur l'équipement concerné.

Réseau informatique : Infrastructure technique permettant l'interconnexion des équipements informatiques de l'établissement afin de partager des ressources (fichiers, imprimantes, accès internet, etc.) et d'échanger des données entre utilisateurs.

Sauvegarde / archivage : La sauvegarde désigne la copie régulière et sécurisée des données en vue de permettre leur restauration en cas de perte, de panne ou d'incident. L'archivage désigne quant à lui la conservation à long terme de données qui ne sont plus en usage courant mais dont la valeur juridique, administrative ou historique justifie la conservation. Ces deux opérations sont complémentaires et relèvent de la responsabilité partagée de l'utilisateur et du service informatique.

Serveurs, routeurs et connectique : Les serveurs sont des équipements informatiques centralisant des services ou des données accessibles aux utilisateurs du réseau. Les routeurs assurent l'acheminement des données entre les différents réseaux. La connectique désigne l'ensemble des câbles, prises et équipements physiques assurant les liaisons entre ces composants.

Service informatique : Entité interne de l'établissement chargée de la gestion, de la maintenance et de la sécurité du système d'information et des ressources informatiques. Il est responsable de l'attribution des droits d'accès, de la mise en œuvre des règles de sécurité et du respect de la présente charte. Ses membres sont soumis à une obligation de confidentialité sur les informations auxquelles ils sont amenés à accéder dans l'exercice de leurs fonctions.

Système d'information (SI) : Ensemble des ressources humaines, matérielles et logicielles permettant de collecter, stocker, traiter et diffuser les informations nécessaires au fonctionnement de l'établissement. Il inclut notamment les équipements informatiques, les logiciels, les données et les réseaux de communication.

Tentative d'intrusion : Toute action non autorisée visant à accéder, modifier ou détruire des ressources du système d'information de l'établissement, qu'elle soit d'origine interne ou externe. Les tentatives d'intrusion sont détectées et tracées par les dispositifs de surveillance du réseau.

Utilisateur : Toute personne physique autorisée à accéder au système d'information et aux ressources informatiques de l'établissement, quel que soit son statut (personnel enseignant, personnel administratif, personnel de direction, etc.). L'utilisateur s'engage à respecter les règles définies par la présente charte dès lors qu'il accède au système d'information, que ce soit depuis les locaux de l'établissement ou à distance.

Virus : Programme informatique malveillant conçu pour s'introduire dans un système d'information à l'insu de l'utilisateur, se reproduire et perturber le fonctionnement des équipements, corrompre ou détruire des données, ou encore ouvrir des accès non autorisés au système. Il se propage généralement via des pièces jointes, des téléchargements ou des supports amovibles infectés.