

CONSEIL REGIONAL ILE-DE- FRANCE

CHARTRE D'UTILISATION

**des systèmes d'information
et des services numériques
au sein des Lycées**

SOMMAIRE

1.	Préambule	4
2.	Définitions	4
3.	Objet	5
4.	Portée et opposabilité de la charte	6
5.	Champ d'application	6
5.1	Personnes concernées	6
5.2	Moyens concernés	6
5.3	Usages concernés	7
6.	Mise à disposition des équipements pédagogiques	7
6.1	Remise des équipements pédagogiques	7
6.2	Règles générales d'utilisation de l'équipement pédagogique	7
6.3	Assistance et maintenance	8
6.4	Durée du prêt et modalités de restitution de l'équipement pédagogique	9
7.	Conditions d'accès et d'identification	9
7.1	Règles générales	9
7.2	Perte ou vol	11
7.3	Modification/suspension des accès	11
8.	Perte et vol de matériel	12
9.	Conditions d'utilisation	12
9.1	Qualité des services numériques et outils informatiques	12
9.2	Utilisation loyale et licite	12
10.	Protection de la propriété intellectuelle	13
11.	Protection des données à caractère personnel	14
11.1	Responsabilités et finalités des traitements	14
11.2	Base juridique des traitements	15
11.3	Destinataires des données	15
11.4	Durée de conservation des données	15
11.5	Flux transfrontières	15

11.6	Vos droits sur les données	16
11.7	Exercice de vos droits	16
12.	Sites internet, produits et services tiers	17
13.	Sécurité et vigilance	17
13.1	Sécurité	17
13.2	Traçabilité	18
13.3	Filtrage	19
13.3.1	Filtrage d'accès Internet	19
13.3.2	Filtrage de Monlycee.net	19
13.4	Scan informatique	19
13.5	Modération des contenus	20
14.	Maintenance	20
15.	Contrôle et audit	21
16.	Responsabilité et sanctions	22

1. Préambule

1. La Région Île-de-France (ci-après « la Région ») met à disposition des utilisateurs différentes ressources et contenus numériques, notamment à travers Monlycée.net (espace numérique de travail qui permet un accès unifié et sécurisé à un ensemble de services et de ressources numériques), la fourniture de postes d'ordinateur et équipements numériques et d'un accès à internet via le réseau Wi-Fi ou filaire des établissements. Cette initiative vise à encourager les transformations pédagogiques et les évolutions de services numériques.
2. L'objectif est de fournir aux utilisateurs les outils permettant les échanges entre les membres de la communauté éducative. Ces outils sont utilisés dans un cadre scolaire, à des fins éducatives et pédagogiques.
3. C'est dans ce cadre que la Région a rédigé la présente charte dont l'objet est de fixer les règles d'utilisation de l'ensemble des services numériques et outils informatiques mis à disposition des différents utilisateurs.
4. Cette charte vise à garantir un usage loyal, respectueux et responsable des services numériques et outils informatiques mis à disposition des utilisateurs.
5. La présente charte n'a pas pour objectif de couvrir de façon exhaustive tous les cas de figure susceptibles de se présenter mais c'est dans l'esprit des règles ci-dessous que chacun devra se positionner dans des situations non envisagées.

2. Définitions

6. Les termes définis ci-après ont la signification suivante :
 - « utilisateur » : désigne de manière générale l'ensemble des personnes physiques, utilisateurs des services numériques et outils informatiques mis à disposition des lycées par la Région tels que visés à l'article 5.1 des présentes. Lorsqu'ils sont mineurs ou majeurs protégés, « utilisateur » désigne les mineurs et majeurs protégés et leurs représentants légaux ;
 - « administrateur » : désigne les membres du personnel auxquels sont attribués des droits étendus permettant notamment de paramétrer l'accès des utilisateurs aux services numériques et de modérer les contenus publiés sur les services numériques ;
 - « établissement » : désigne le lycée de la Région Île-de-France ou autre établissement public d'enseignement dont la Région a la tutelle, auquel est rattaché l'utilisateur ;
 - « services numériques » : désigne l'ensemble des ressources et contenus numériques mis à la disposition des utilisateurs, notamment à travers Monlycée.net ainsi que l'accès au réseau Wi-Fi ou filaire des établissements ;
 - « outils informatiques » : il s'agit de postes d'ordinateur et de tablettes graphiques et numériques et autres supports multimédia ainsi que les applications et logiciels installés par la Région ;

- « équipement pédagogique » : il s'agit des équipements numériques mis à disposition des élèves, des enseignants et des personnels non-enseignants des lycées d'Île-de-France par la Région ;
- « donnée à caractère personnel » : désigne toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une « personne physique identifiable » toute 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 ;
- « filtrage » : ensemble d'outils informatiques visant à limiter l'accès à certains sites Internet en raison de leurs contenus (contrôle des contenus, des URL, protocoles, etc.) ;
- « matériel nomade » : moyens informatiques et de communication électronique portables, pouvant en conséquence être utilisés à l'extérieur de l'établissement auquel est rattaché l'utilisateur ;
- « moyen d'authentification » : moyen permettant l'accès aux systèmes d'information et de communication et pouvant prendre diverses formes : identifiant/mot de passe, , signature électronique, badges, cartes avec ou sans contact, etc. ;
- « RGPD » : désigne le règlement (UE) du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données personnelles et à la libre circulation de ces données ;
- « service en ligne » : service de communication par voie électronique de mise à disposition du public ou de catégories de public, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondance privée ;
- « trace informatique » ou « trace » : donnée informatique témoignant de l'existence d'une opération au sein d'une application ou des systèmes d'information et de communication ;
- « logiciel malveillant » : logiciel développé dans le but de nuire à un système informatique (virus, vers, chevaux de Troie, keyloggers, rançongiciels, etc.).

3. **Objet**

7. La présente charte a pour objet de fixer les règles d'utilisation de l'ensemble des services numériques et outils informatiques mis à la disposition par la Région au profit des utilisateurs.
8. Elle a également pour objet de définir l'ensemble des principes, règles, méthodes et procédures qui forment le socle commun des meilleures pratiques en matière d'utilisation des moyens informatiques et de communication électronique.

9. La présente charte, pourra, le cas échéant, être complétée de documents spécifiques (charte d'utilisation, manuel utilisateur, règlement intérieur ou autres) en fonction des outils, services et espaces en question¹.

4. Portée et opposabilité de la charte

10. La présente charte est opposable à tous les utilisateurs. Elle peut être annexée au règlement intérieur des lycées.
11. La Région se réserve le droit de conditionner l'accès aux services numériques et outils informatiques par l'acceptation de la présente charte et ses versions ultérieures, par les utilisateurs.
12. Cette acceptation s'effectue via une case à cocher lors de la première connexion des utilisateurs au service numérique Monlycée.net.
13. Dans le cas où l'utilisateur est mineur, la charte doit également être acceptée par le ou les parents ou le représentant légal du mineur.
14. En tout état de cause, cette acceptation n'est pas une condition nécessaire à l'opposabilité de la charte.
15. La présente charte est un document évolutif, pouvant faire l'objet de dispositions nouvelles, rendues opposables par publicité préalable sur le site Monlycée.net.
16. La version de la charte opposable est celle consultable en ligne ou par voie d'affichage au moment de l'utilisation des services numériques et outils informatiques mis à disposition par la Région.

5. Champ d'application

5.1 Personnes concernées

17. La présente charte est applicable, et donc opposable, à tout utilisateur autorisé à accéder aux services numériques et outils informatiques mis à disposition par la Région, quel que soit son statut (élèves des lycées, parents d'élèves des lycées, agents des lycées, agents de l'éducation nationale enseignants et non enseignants, stagiaires, partenaires, membres des conseils d'administration des lycées).

5.2 Moyens concernés

18. Est visé par la présente charte l'ensemble des services numériques et outils informatiques mis à la disposition des utilisateurs par la Région et notamment, sans que cette liste ne soit exhaustive, les outils, services et espaces suivants :
- ordinateurs fixes;
 - ordinateurs portables ;

¹ Les agents de la Région sont également soumis à la charte pour l'usage des ressources informatiques et des services internet de la Région.

- tablettes graphiques et numériques ;
- moyens informatiques et de communication électronique ;
- tableaux numériques ;
- disques durs externes ;
- Wi-Fi ;
- accès internet filaire ;
- place des services numériques « MonLycée.net ».

5.3 Usages concernés

19. La présente charte s'applique à tous les types d'usage, qu'il s'agisse d'un usage à titre privé ou professionnel de l'utilisateur et qu'ils aient lieu :
- dans les locaux de l'établissement des utilisateurs ;
 - dans le cadre d'un usage dit « nomade », quel qu'en soit le lieu ;
 - dans le cadre d'un accès distant, quel que soit le lieu de cet accès (domicile, etc.).

6. Mise à disposition des équipements pédagogiques

20. Cet article a pour objet de définir les conditions de mise à disposition des équipements pédagogiques aux utilisateurs ainsi que les conditions de détention et d'usage de ces équipements.

6.1 Remise des équipements pédagogiques

21. La remise de l'équipement pédagogique est soumise à l'acceptation préalable de la présente charte. Les conditions du prêt doivent être acceptées par les élèves et une attestation de remise signée par les enseignants et personnels. Ces conditions sont acceptées sans réserve par l'utilisateur doté d'un équipement et, lorsqu'il s'agit d'un élève mineur, par son ou ses représentants légaux. L'équipement pédagogique est mis à disposition de l'utilisateur à titre individuel et nominatif.
22. L'équipement pédagogique est remis à l'utilisateur par son établissement. Il est identifiable par un numéro de série et fait l'objet d'un enregistrement informatisé au moment de la remise à l'utilisateur.
23. L'équipement n'est pas la propriété de l'utilisateur ou de son représentant mais celle de la Région. La revente, la cession, même à titre gratuit, l'échange, le prêt ou la location de l'équipement sont strictement interdits.

6.2 Règles générales d'utilisation de l'équipement pédagogique

24. Pour tout utilisateur, l'activation de son compte Monlycée.net et la saisie de ses identifiants et mot de passe est nécessaire pour pouvoir utiliser l'équipement pédagogique.
25. L'utilisateur peut y stocker des données personnelles dans la mesure où le volume de ces données ne nuit pas à la performance de l'équipement. L'espace de stockage disponible sur l'équipement étant limité, l'utilisateur est informé qu'il peut lui être demandé de supprimer de l'équipement pédagogique des contenus personnels trop volumineux.
26. L'élève s'engage à :

- toujours avoir son équipement chargé en état d'usage lorsqu'il arrive dans l'établissement ;
- conserver et prendre soin de l'équipement confié, dont il est le gardien. Son ou ses représentants légaux sont garants de ces obligations.

27. Hors temps scolaire, l'élève, sous le contrôle de son ou ses représentants légaux, peut utiliser l'équipement pour des usages ludiques ou culturels à titre personnel.
28. Toute connexion à internet effectuée en dehors de l'établissement que ce soit au domicile de l'élève ou depuis tout autre point d'accès, même public, relève de l'entière responsabilité du ou des représentants légaux.
29. Les nouveaux équipements mis à disposition depuis [date à préciser] disposent d'une fonctionnalité de contrôle parental permettant aux représentants légaux des élèves de contrôler l'accès à certaines applications disponibles sur l'ordinateur au domicile ainsi que de suivre et bloquer des sites web.
30. Cette application de contrôle parental peut être activée ou désactivée par les représentants légaux de l'élève.
31. En cas de non-respect des présentes conditions du prêt, l'utilisateur s'expose à une confiscation de l'équipement pédagogique matériel ainsi qu'à des sanctions disciplinaires.

6.3 Assistance et maintenance

32. **Panne.** Tout problème technique doit immédiatement être signalé au service de support <https://assistanceidf.zendesk.com/hc/fr>.
33. En cas de panne, l'utilisateur doit indiquer précisément au support dans quelles circonstances la panne est intervenue. Elle sera prise en charge par le support dans le cadre de la garantie de l'équipement. L'équipement pédagogique est traité et remis à disposition dans les meilleurs délais.
34. Aucune intervention externe n'est autorisée sur l'équipement pédagogique. Toute intervention externe entraînera un arrêt de la garantie de l'équipement qui ne pourra plus être pris en charge par le service de support technique.
35. **Obligation de soin et endommagement de l'équipement pédagogique.** L'utilisateur doit prendre toutes les précautions nécessaires pour éviter toute dégradation, usage abusif ou vol de l'équipement pédagogique. L'élève et ses représentants légaux ont une obligation de soin à l'égard de l'équipement pédagogique prêté.
36. Un état des endommagements des équipements pédagogiques par utilisateur est établi par Unowhy. Cet état vise nommément les utilisateurs concernés.
37. Les équipements sont classés selon une gradation (A, B, C, D, HC) qui détermine le choix des équipements de remplacement à fournir aux utilisateurs par ordre de priorité.
38. À titre d'exemple, en cas d'endommagement ou de vol d'un équipement 2023 de grade A, celui-ci est remplacé par un équipement 2023 de même grade s'il en existe un de disponible,

ou à défaut un équipement 2023 de grade B, ou à défaut un équipement 2022 de grade A ou à défaut un équipement 2022 de grade B.

39. Il en résulte qu'un utilisateur à l'origine de plusieurs endommagements est susceptible de recevoir un équipement doté d'un grade inférieur. Selon les équipements disponibles et l'ordre de priorité, l'utilisateur ne pourrait plus bénéficier de la mise à disposition d'équipement pédagogique.
40. L'utilisateur s'engage à informer la Région de toute perte, anomalie de l'équipement pédagogique. L'utilisateur reconnaît avoir été informé qu'en cas de perte, vol ou dégradation autre que celle liée à l'usage conforme de ces matériels, sa responsabilité civile pourra être engagée.
41. En cas de perte, de casse ou de vol, le remplacement de l'équipement pédagogique n'est pas un droit acquis et relève de l'examen de chaque situation.

6.4 Durée du prêt et modalités de restitution de l'équipement pédagogique

42. L'équipement pédagogique est mis à disposition de l'élève (et de son représentant légal) jusqu'à la fin de sa scolarité secondaire. Par la suite, il peut en devenir propriétaire ou décider de le rendre à l'établissement afin qu'il soit reconditionné.
43. L'élève (et son représentant légal) s'engage à restituer sans délai l'équipement pédagogique prêté en cas de départ définitif d'un établissement de la Région Île-de-France avant la fin de sa scolarité. La procédure de retour de l'équipement pédagogique sera indiquée à l'élève (et son représentant) par l'établissement.
44. Si l'élève choisit de garder l'équipement pédagogique, celui-ci est déconnecté de l'application de suivi des équipements MDM et du logiciel Azure AD pour permettre à l'élève d'en disposer librement. Les comptes ouverts sur Azure AD sont supprimés deux fois par an, en janvier et en juin.
45. Jusqu'à la fin de leur garantie, les équipements peuvent encore faire l'objet d'une demande de service après-vente par les élèves.
46. Pour les enseignants et le personnel non-enseignant, l'équipement pédagogique est mis à disposition tant qu'ils restent affectés dans un lycée francilien.

7. Conditions d'accès et d'identification

7.1 Règles générales

47. Chaque utilisateur dispose d'un ou de plusieurs moyens d'authentification permettant l'accès aux services numériques et outils informatiques.
48. La politique d'habilitation et de profil au sein du système d'information est déterminée par la Région.

49. Chaque utilisateur se voit attribuer un compte utilisateur accessible avec des identifiants, incluant un code d'activation par défaut. L'utilisateur doit ensuite modifier le mot de passe lors de sa première connexion. Les identifiants et mots de passe créés lors d'une précédente année scolaire au sein du même établissement scolaire sont conservés.
50. Le mot de passe est créé par l'utilisateur dans le respect des critères de sécurité imposés. Il est strictement personnel et confidentiel.
51. L'identification par mot de passe doit répondre aux exigences suivantes :
- utiliser un mot de passe robuste – ne pas utiliser des termes usuels ou en lien direct avec soi (par exemple noms des conjoints, date de naissance, surnom des enfants, animaux, ...) – ne pas utiliser de suites ou de répétitions de caractères (exemple : azerty, aaaa, 1234, etc.) – ne pas utiliser des termes du dictionnaire français ou étranger ;
 - utiliser un mot de passe d'au moins 12 caractères de 4 types différents (majuscules, minuscules, chiffres, caractères spéciaux) ;
 - l'interdiction d'utiliser le même mot de passe pour des accès différents ;
 - ne pas utiliser son identifiant comme mot de passe ;
 - ne pas reprendre un mot de passe déjà utilisé dans le passé ;
 - ne pas afficher ou inscrire son mot de passe en clair quel que soit l'endroit ou la forme (ne le notez pas sous le clavier ou sur le côté de l'écran) ;
 - taper son mot de passe à l'abri du regard de tiers ;
 - ne pas cocher « enregistrement du mot de passe » ou « save password » dans les navigateurs utilisés.
52. Il est, dès lors, interdit à l'utilisateur :
- de partager son ou ses moyens d'authentification (identifiant et mot de passe) ;
 - d'utiliser un identifiant et un mot de passe autres que les siens ;
 - de supprimer, masquer ou modifier son identité ou son identifiant.
53. L'accès à Monlycée.net est soumis à une identification préalable de l'utilisateur qui dispose d'un identifiant et d'un mot de passe strictement personnels et confidentiels.
54. Dans le cadre de Monlycée.net, une adresse de messagerie électronique, composée de [prénom].[nom]@monlycee.net est attribuée à chaque utilisateur.
55. L'adresse de messagerie est destinée aux échanges dans le cadre de la communauté éducative. Elle sera supprimée trois mois après la fin de la scolarisation ou de l'affectation de l'utilisateur dans un établissement francilien.

56. En termes de sécurité et de confidentialité, l'utilisateur doit suivre les recommandations faites par la Région ou son établissement.
57. L'utilisateur s'engage notamment à ne jamais quitter un outil informatique sans s'être déconnecté de Monlycée.net.
58. L'utilisateur s'engage à signaler dans les plus brefs délais toute utilisation frauduleuse de son compte, de son identifiant ou de son mot de passe dont il aurait connaissance à l'adresse de mél officielle de son établissement et aussi à dpo@iledefrance.fr.
59. Tout usage des services numériques et outils informatiques est imputé à l'utilisateur bénéficiaire du moyen d'authentification utilisé. L'utilisateur en assume donc toute conséquence, notamment juridique et financière, sauf s'il a engagé préalablement une demande de suspension ou de suppression d'autorisation, ou s'il est en mesure de démontrer qu'il n'est pas responsable de ces usages.

7.2 Perte ou vol

60. Si ces moyens d'authentification ont fait l'objet d'une communication à des tiers, ou qu'il existe un risque qu'ils soient communiqués, ou qu'ils aient été communiqués à des tiers ou captés par eux, à la suite notamment de leur perte, de leur vol ou encore de leur oubli, l'utilisateur concerné doit, sans délai :
 - renouveler ses moyens d'authentification et, s'il rencontre des difficultés lors de cette opération de renouvellement contacter son chef d'établissement;
 - dans tous les cas, informer son Chef d'établissement ou son supérieur hiérarchique de cette perte ou de ce vol;
 - selon le cas, porter sa meilleure assistance à son chef d'établissement et à la Région lorsque ces derniers doivent mener des démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'incidents liés à la perte ou le vol de ses moyens d'authentification et cela quelle que soit la nature de ces incidents, ou réaliser, lui-même, ces démarches, notamment au dépôt de plainte.

7.3 Modification/suspension des accès

61. En cas de suspicion de compromission de son identifiant et mot de passe, l'utilisateur est tenu d'en informer sans délai son chef d'établissement ou supérieur hiérarchique ou le référent numérique de son établissement. Seul cet acte d'information peut dégager la responsabilité de l'utilisateur pour les agissements qui auraient lieu suite à sa déclaration.
62. La Région se réserve, lorsque la situation le justifie, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer en tout ou partie, le droit d'accès de toute personne aux systèmes d'information et de communication.
63. La Région s'efforcera, autant que faire se peut, de prévenir l'utilisateur concerné, dans des délais raisonnables, notamment en cas de maintenance.

8. Perte et vol de matériel

64. En cas de perte ou de vol de matériel informatique, l'utilisateur informera immédiatement son chef d'établissement ou supérieur hiérarchique ou le référent numérique de son établissement.
65. En cas de perte d'un matériel mis à disposition de l'utilisateur, ce dernier fournira un rapport circonstancié par écrit et établira une main courante auprès des services de police ou de gendarmerie.
66. En cas de vol d'un matériel mis à disposition de l'utilisateur, l'utilisateur fournira un rapport circonstancié par écrit et devra déposer plainte auprès des services de police ou de gendarmerie et transmettra une copie du dépôt de la plainte à equipements.numeriques@iledefrance.fr.
67. En cas d'usurpation d'identité avérée, l'utilisateur adressera un courriel à dpo@iledefrance.fr.
68. En tout état de cause, l'utilisateur devra aider la Région à mettre en œuvre les démarches nécessaires, notamment pour empêcher l'accès aux données personnelles accessibles via le matériel informatique concerné.
69. En fonction de la disponibilité des stocks, la direction des systèmes d'information et d'organisation procèdera au remplacement des matériels au mieux.

9. Conditions d'utilisation

9.1 Qualité des services numériques et outils informatiques

70. Les conditions d'utilisation sont définies par la Région en fonction des services numériques et outils informatiques mis à disposition par la Région.
71. La Région fait ses meilleurs efforts pour assurer l'accès aux services numériques et outils informatiques qu'elle met à disposition, sans pouvoir garantir une accessibilité permanente.
72. La Région ne saurait ainsi être responsable :
 - de la qualité des services numériques et des outils informatiques, ceux-ci étant proposés « en l'état » ;
 - d'une perturbation, d'une indisponibilité temporaire ou de l'impossibilité d'utiliser le réseau Wi-Fi ou filaire ou l'un des services numériques ou l'un des outils informatiques ;
 - d'une difficulté liée au temps de réponse ou d'un défaut de performance quelconque.

9.2 Utilisation loyale et licite

73. Les outils et services sont mis à la disposition des utilisateurs dans un cadre scolaire, à des fins éducatives et pédagogiques.
74. L'utilisateur s'engage à effectuer une utilisation normale et raisonnable des services numériques et outils informatiques, dans le respect de la présente charte en agissant conformément aux législations et réglementations en vigueur, à l'ordre public, aux bonnes

mœurs et aux droits des tiers notamment, dans le respect des lois et réglementations relatives :

- à la propriété littéraire et artistique ;
- à l'informatique, aux fichiers et aux libertés ;
- à la protection de la vie privée et du droit à l'image d'autrui ;
- aux droits de l'homme en s'assurant de ne pas envoyer de messages à caractère raciste, terroriste, pornographique, pédophile, injurieux, diffamatoire et de manière générale à ne pas diffuser d'informations présentant un caractère délictueux.

75. L'utilisateur s'interdit tout comportement illégal, illicite ou constitutif d'une fraude à l'égard de la Région ou des autres utilisateurs ou des tiers.
76. L'utilisateur garantit la Région contre l'altération, la détérioration ou l'endommagement des services numériques.
77. Dans cet esprit, il s'engage notamment à :
- prendre soin des services et outils mis à sa disposition ;
 - ne pas interrompre le fonctionnement normal des outils ou services mis à sa disposition ;
 - ne pas contourner les systèmes de sécurité ;
 - ne pas introduire de programmes malveillants : virus, espions ou nuisibles ;
 - ne pas installer de logiciel ou application (mobile ou non) sans l'autorisation de la Région.

10. Protection de la propriété intellectuelle

78. L'utilisation des services numériques et des outils numériques mis à disposition par la Région implique le respect des droits de propriété intellectuelle.
79. Le contenu, la structure générale ainsi que les marques, les dessins, les modèles, les images animées ou non, les textes, les photographies, les logos, les chartes graphiques, les logiciels et programmes, les moteurs de recherche, les bases de données, les sons, les vidéos, les noms de domaines de la Région et tous les autres éléments composant les services numériques et outils informatiques mis à disposition ou toute autre information, sans que cette liste ne soit exhaustive, sont la propriété exclusive de la Région ou des tiers qui lui ont concédé une licence, et sont protégés par des droits de propriété intellectuelle qui leur sont ou seront reconnus selon les lois en vigueur.
80. La mise à disposition des services numériques et des outils numériques par la Région ne confère aucun droit de propriété ou de licence ou aucun droit sur ces services et outils au bénéfice de l'utilisateur autre que le droit d'utilisation des services numériques et outils informatiques de façon conforme à la présente charte.
81. Sans que cette liste soit exhaustive, l'utilisateur s'engage à :
- utiliser les logiciels, applications, dans le respect des conditions posées par la Région ;
 - ne pas effectuer de copie illicite de logiciel, d'applications et, a fortiori, de tenter d'installer des logiciels pour lesquels la Région ne posséderait pas un droit d'usage ;
 - ne pas reproduire et utiliser les bases de données, pages web ou autres créations de la Région ou de tiers protégés par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;

- ne pas diffuser des textes, des images, des photographies, des œuvres musicales ou audiovisuelles et, plus généralement, toute création copiée sur le réseau internet sans autorisation du titulaire des droits ;
- ne pas copier et remettre à des tiers des créations appartenant à des tiers ou à la Région sans s'assurer de l'autorisation du titulaire des droits qui s'y rapporte.

82. En conséquence, l'utilisateur s'interdit tout agissement et tout acte susceptible de porter atteinte directement ou non aux droits de propriété intellectuelle de la Région.

11. Protection des données à caractère personnel

11.1 Responsabilités et finalités des traitements

83. Une partie des traitements mis en œuvre dans le cadre des usages numériques au sein des lycées a pour seul responsable de traitement la Région Île-de-France

84. Concernant les traitements spécifiques relatifs au dispositif Monlycée.net, le chef d'établissement, l'Académie et la Région Île-de-France sont responsables de traitement conjoints en ce qu'ils ont défini ensemble les finalités et moyens principales du traitement tel que décrit ci-après.

85. Les moyens matériels, logiciels et de ressources humaines affectés à la gestion du traitement sont définis de manière conjointe par le chef d'établissement, l'Académie et la Région.

86. La durée de conservation des données est définie par la Région. Les mesures de sécurité, d'accès et de traçabilité sont définies conjointement par l'Académie et la Région.

87. L'Académie et la Région définissent les catégories de données traitées ou le choix des données traitées dans le cadre de la mise à disposition de Monlycée.net.

88. Le chef d'établissement est responsable des données traitées dans le cadre de l'utilisation courante de Monlycée.net par la communauté éducative.

89. **Traitements mis en œuvre uniquement par la Région.** En tant que responsable de traitement, la Région met en œuvre un traitement de données concernant les utilisateurs ayant les finalités suivantes :

- assurer le fonctionnement des lycées et mettre à disposition les matériels informatiques (et les logiciels prévus pour leur mise en service) nécessaires à l'enseignement et aux échanges entre les membres de la communauté éducative (art. L214-6 code de l'éducation) à l'exclusion du dispositif Monlycée.net ;
- la gestion de la sécurité, le bon fonctionnement des services numériques et outils informatiques et la détection et la résolution d'incidents ou de problèmes liés à son utilisation ;
- la gestion du prêt d'équipements numériques aux élèves, aux enseignants et aux personnels non-enseignants;
- la gestion des enquêtes auprès des utilisateurs de Monlycée.net ;
- le respect de la présente charte.

90. **Traitements mis en œuvre conjointement par le chef d'établissement, l'Académie et la Région Île-de-France.** En tant que responsables de traitement conjoints, le chef

d'établissement, l'Académie et la Région Île-de-France mettent en œuvre un traitement ayant pour finalité la gestion du dispositif Monlycée.net.

91. Dans ce cadre, les données des utilisateurs sont collectées à des fins pédagogiques et administratives afin de donner accès aux utilisateurs au dispositif Monlycée.net et dans le cadre de leur utilisation de ce dernier.
92. Les responsables de traitement mettent en œuvre les traitements nécessaires à l'enseignement, aux échanges entre les membres de la communauté éducative, à la mise à disposition de contenus éducatifs et pédagogiques ou relatives à la vie scolaire, à la gestion des comptes utilisateurs. Un outil de marquage permet d'établir des statistiques de fréquentation des différents services de l'ENT et de les croiser avec les profils utilisateurs

11.2 Base juridique des traitements

93. Le fondement juridique des traitements est l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement en application des articles L214-6, R222-24-2 et L421-3 du code de l'éducation.

11.3 Destinataires des données

94. **Traitements mis en œuvre uniquement par la Région.** Les données collectées sont destinées aux membres du personnel habilités de la Région et dans les limites du besoin d'en connaître pour les nécessités du service, aux membres du personnel habilités de ses sous-traitants et les autorités légales dans le cadre de demandes officielles.
95. **Traitements mis en œuvre conjointement par le chef d'établissement, l'Académie et la Région Île-de-France.** Les données collectées sont destinées aux membres du personnel habilités de la Région ainsi qu'aux personnels habilités des lycées et de l'Académie dans le cadre strict de leurs attributions et dans les limites du besoin d'en connaître pour les nécessités du service.

11.4 Durée de conservation des données

96. Les données sont conservées jusqu'à trois mois après la fin de la scolarisation ou de l'affectation de l'utilisateur dans un établissement francilien. Les données de connexion sont conservées pour une durée d'un an à compter de leur collecte.
97. Si un contenu créé par un utilisateur a plusieurs gestionnaires, ce dernier ne sera supprimé que lors de la suppression du compte du dernier gestionnaire.
98. Dans le cadre spécifique de la gestion des enquêtes auprès des utilisateurs, les données sont conservées pendant la durée indiquée aux utilisateurs dans l'enquête elle-même.

11.5 Flux transfrontières

99. Certaines données sont susceptibles d'être transférées pour des cas légitimes et encadrés, en dehors de l'Union européenne, en particulier vers les Etats-Unis dans le cadre de l'utilisation des outils Microsoft.

100. Ces transferts sont encadrés par une décision d'adéquation de la Commission européenne ainsi que la mise en place des clauses contractuelles types de la Commission européenne. Vous pouvez obtenir une copie de ces garanties en vous adressant à notre délégué à la protection des données à l'adresse indiquée ci-dessous.

11.6 Vos droits sur les données

101. Les utilisateurs disposent d'un droit d'accès, de rectification, d'effacement, ainsi que d'un droit à la limitation du traitement.

102. Ils disposent également du droit de s'opposer à tout moment, pour des raisons tenant à leur situation particulière, à un traitement des données à caractère personnel ayant comme base juridique l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique ou la réalisation des intérêts légitimes poursuivis par la Région.

103. Les utilisateurs disposent du droit de formuler des directives générales ou particulières concernant la conservation, l'effacement et la communication des données post-mortem les concernant.

104. Les utilisateurs disposent du droit d'introduire une réclamation auprès de la Commission nationale Informatique et Libertés.

11.7 Exercice de vos droits

105. **Traitements mis en œuvre uniquement par la Région.** Les demandes relatives à l'exercice de leurs droits s'effectuent auprès du délégué à la protection des données de la Région dont les coordonnées sont précisées ci-dessous.

106. Les utilisateurs peuvent contacter la Région en tant que responsable de traitement et son délégué à la protection des données à l'adresse mail suivante : dpo@iledefrance.fr et à l'adresse postale suivante : Région Île-de-France, Pôle Transformation Numérique, à l'attention du Délégué à la Protection des Données, 2 rue Simone Veil 93400 Saint-Ouen-sur-Seine.

107. **Traitements mis en œuvre conjointement par le chef d'établissement, l'Académie et la Région Île-de-France** L'utilisateur exerce ses droits auprès du chef d'établissement qui en informera immédiatement l'Académie et la Région en cas de nécessité.

108. Si l'utilisateur estime, après avoir saisi le chef d'établissement, que la réponse apportée n'est pas satisfaisante, il peut s'adresser aux délégués à la protection des données des responsables conjoints du traitement aux adresses suivantes :

- dpd@ac-creteil.fr pour l'Académie de Créteil ;
- dpd@ac-paris.fr pour l'Académie de Paris ;
- dpd@acversailles.fr pour l'Académie de Versailles ;
- dpo@iledefrance.fr pour la Région Île-de-France.

109. L'ensemble des délégués à la protection des données désignés collaborent ensemble dans le cadre des traitements de données dont le chef d'établissement, l'Académie et la Région sont responsables conjoints.

Pour plus d'informations sur la protection de leurs données à caractère personnel, les utilisateurs peuvent se référer à la fiche pédagogique relative à la protection des données personnelles des élèves [ici](#).

12. Sites internet, produits et services tiers

110. Les services numériques peuvent inclure des liens vers, ou appeler les serveurs de sites internet ou de services tiers qui échappent au contrôle de la Région.
111. La Région n'est pas responsable et n'offre aucune garantie liée aux informations ou ressources contenues dans les services tiers ou accessibles via ces derniers.
112. De même, la Région n'est pas responsable de tout dysfonctionnement des services tiers.
113. L'utilisateur est invité à consulter les conditions générales d'utilisation et les conditions applicables à l'accès et à l'utilisation de ces services tiers avant toute utilisation.

13. Sécurité et vigilance

13.1 Sécurité

114. Les services numériques et outils informatiques mis à disposition constituent un système de traitement automatisé de données. Il est interdit d'y accéder ou de s'y maintenir, frauduleusement.
115. En cas de découverte d'une telle méthode ou si l'utilisateur entre dans un espace réservé, sans droit, par inadvertance, celui-ci s'engage à en informer sans délai le référent numérique de l'établissement et par courrier électronique la Région à l'adresse rsi@iledefrance.fr afin qu'elle puisse prendre les mesures nécessaires.
116. Le réseau Wi-Fi mis à la disposition des utilisateurs présente les mêmes caractéristiques que les connexions internet standard.
117. A des fins de précaution, certaines configurations peuvent être verrouillées par la Région (poste de travail, accès internet, etc.).
118. De même certains services ou outils peuvent être protégés par une serrure ou un cadenas.
119. La mise en place d'outils de sécurité par la Région ne doit pas, toutefois, dispenser les utilisateurs d'une obligation de vigilance à cet égard.
120. C'est pourquoi, l'utilisateur :
 - doit prendre toutes mesures appropriées de façon à assurer sa propre sécurité, et à protéger ses propres données et / ou logiciels de la contamination par d'éventuels codes malveillants sur le réseau internet ;
 - ne doit pas contourner ou désactiver ou tenter de contourner ou de désactiver des mesures de sécurité installées par la Région.
121. En effet, tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des outils et des services mis à sa disposition, principalement en évitant les intrusions physiques le cas échéant,

mais aussi l'introduction de codes malveillants susceptibles d'endommager le système d'information de la Région ou tout autre système d'information.

122. L'utilisateur s'interdit également de :

- modifier les services numériques et outils informatiques mis à sa disposition notamment par l'ajout de logiciels, progiciels, même gratuits, ou de matériels pour quelque raison que ce soit, sans autorisation des personnels habilités ;
- modifier ou détruire, ou tenter de modifier ou détruire, des fichiers sur lesquels il ne dispose d'aucun droit, en particulier les fichiers contenant des informations comptables ou d'identification ;
- mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont il a usage ;
- utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ou masquer son identité ;
- effectuer des opérations pouvant nuire aux relations internes ou externes de la Région ;
- de quitter les espaces mis à sa disposition sans en verrouiller l'accès le cas échéant.

123. En cas de réception de messages non sollicités (spams), l'utilisateur veille à :

- ne pas l'ouvrir sans s'être assuré préalablement de son caractère inoffensif ;
- ne pas y répondre ;
- ne pas le transférer.

13.2 Traçabilité

124. Au titre de ses obligations légales et réglementaires du fait de la fourniture des services numériques et outils informatiques, la Région conserve les données d'identification et de connexion des utilisateurs dont elle assure la protection, l'intégrité et la confidentialité. Cette conservation ne peut excéder une durée d'un an.

125. La traçabilité a pour but de pouvoir reconstituer l'historique des opérations effectuées sur un système d'information. La traçabilité est rendue nécessaire par des considérations de natures diverses et notamment :

- juridiques : augmenter les chances de rendre opposables des preuves établies par voie électronique ;
- métier : offrir de nouveaux services ;
- techniques : suivre la qualité de service offerte ;
- organisationnelles : mettre en œuvre les ressources et les procédures adéquates.

126. L'ensemble des applications et accès génère des traces informatiques. De même l'utilisation des outils de communication électronique génère des données de connexion ou des données de trafic.

127. Ces données peuvent être exploitées sous toute forme et notamment sur la forme de logs et journaux d'historisation.

128. Les données collectées sont généralement les suivantes, sans que cette liste soit exhaustive :

- identité de l'utilisateur ;
- heure de connexion//déconnexion ;
- navigation ;
- type de matériel ;
- date.

13.3 Filtrage

13.3.1 Filtrage d'accès Internet

129. Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité de tenter de prévenir tout usage illicite de ses systèmes d'information et de communication, la Région met en place des outils de filtrage permettant d'analyser les conditions d'utilisation de ses systèmes, d'interdire tel ou tel protocole, ou encore de restreindre la consultation de certaines catégories de sites internet ou d'applications.
130. Ces outils permettent un contrôle des connexions des utilisateurs car ils portent, entre autres, sur l'accès à internet. Ils permettent notamment de vérifier les accès mais également les tentatives d'accès voire même les tentatives de détournement de la solution.
131. Le résultat de ces traitements, notamment l'analyse des accès Internet, peuvent être rendus publics pour autant qu'ils soient anonymes ou communiqués directement à l'utilisateur pour qu'il puisse remédier à d'éventuels écarts avec les conditions normales d'utilisation.
132. Il est strictement interdit de détourner, d'altérer ou de modifier les outils de filtrage ou les données recueillies grâce à ces outils.

13.3.2 Filtrage de Monlycee.net

133. Monlycée.net est un espace numérique de travail mis à la disposition des utilisateurs permettant notamment de partager du contenu mais dont l'utilisation doit se limiter au cadre scolaire, à des fins éducatives et pédagogiques.
134. Afin de protéger les utilisateurs, la Région se réserve le droit de mettre en place des mesures de filtrage par mots clés afin de bloquer l'envoi ou la diffusion de messages ou contenus illicites.
135. Lorsque qu'un mot clé est identifié, le message ou le contenu est bloqué et l'utilisateur reçoit un message l'informant de ce blocage.
136. Ce type de mesures peut être décidé pour une durée limitée ou permanente en fonction des circonstances et des espaces de Monlycée.net concernés.
137. La liste de mots clés prise en compte pour le filtrage des messages est susceptible d'évoluer selon les besoins de sécurisation de Monlycée.net et les circonstances.

13.4 Scan informatique

138. Le scan informatique consiste à contrôler, à travers des outils informatiques, la présence de mots clés dans des contenus des systèmes d'information et de communication de la Région.

139. La Région peut mettre en œuvre des opérations de scan des systèmes d'information et de communication, tels que le scan des services numériques, et notamment des documents, des dossiers, des messages électroniques, pièces jointes, fichiers.
140. Les outils de scan informatique n'ont pas pour objet l'ouverture des éléments identifiés. Ils permettent à la Région de bénéficier d'un dispositif d'alerte prudentiel, et rapide, de ses systèmes d'information et de communication.
141. Les documents, dossiers, messages électroniques, pièces jointes, etc., identifiés comme « PRIVE » ne seront pas consultés par la Région, sauf dans le cadre des dispositions légales particulières de la jurisprudence en la matière et des dispositions de cette charte.
142. Une liste de mots clés permettant les scans informatiques est déterminée par la Région.

13.5 Modération des contenus

143. La majorité des applications accessibles à partir de Monlycée.net contiennent des zones de saisies libres dans lesquelles des données peuvent être saisies par les utilisateurs.
144. Les utilisateurs ne doivent renseigner que des contenus entrant dans le cadre d'une [Utilisation loyale et licite](#) (telle que décrite à l'article 9.2 de la présente charte) des systèmes d'information et des services numériques et n'être utilisées qu'à des fins éducatives et pédagogiques
145. En particulier, les données saisies dans ces zones doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard de leur objectif. Il convient d'éviter tout commentaire portant sur le comportement ou les traits de caractère d'une personne. Que les informations concernent l'utilisateur ou d'autres personnes, les données relatives à la santé, à la religion, aux opinions politiques, syndicales et philosophiques, aux origines ethniques, ainsi qu'aux sanctions et condamnations ne doivent pas être saisies dans ces zones.
146. La modération des contenus publiés sur Monlycée.net s'effectue via un système de signalement des contenus inappropriés accessible à tous les utilisateurs.
147. Les signalements sont remontés à l'administrateur local au sein de l'établissement de l'utilisateur concerné par la création du signalé, ils précisent l'identité de l'utilisateur à l'origine du signalement.
148. L'administrateur peut alors supprimer la notification relative au contenu publié. Le compte de l'utilisateur à l'origine de la publication du contenu pourra également être bloqué par l'administrateur. S'il l'estime nécessaire le chef d'établissement pourra décider de la suppression du contenu.
149. Si le signalement du contenu n'est pas justifié, ce dernier est ignoré.

14. Maintenance

150. La mise à disposition des services numériques et outils informatiques fournis par la Région implique nécessairement des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, de maintenance préventive ou de maintenance évolutive.

151. L'objectif de ces opérations n'est autre que d'assurer le bon fonctionnement et la sécurité des services numériques et outils informatiques mis à disposition par la Région. Elles se distinguent en cela des opérations de contrôle et d'audit expliquées ci-après.
152. Ces opérations peuvent prendre la forme de « prises de main sur des postes informatiques » effectuées par une « personnes habilitée ». Celle-ci intervient soit sur site, soit à distance.
153. En aucun cas, ces opérations, quel que soit leur mode opératoire, ne justifient le fait pour l'utilisateur de communiquer ses moyens d'authentification.
154. Dans ce cadre, la « personne habilitée » peut être amenée à prendre connaissance de l'ensemble des éléments présent sur le poste de l'utilisateur, ainsi que des données de connexion.
155. Si, à l'occasion d'opérations de maintenance, des utilisations anormales ou des contenus illicites ou préjudiciables sont identifiés, la Région en tirera toute conséquence.
156. La Région se réserve le droit, sans préavis, ni indemnité, d'interdire temporairement l'accès aux services numériques et outils informatiques, notamment pour effectuer une mise à jour, des opérations de maintenance, des modifications ou changements sur les méthodes opérationnelles et fonctionnalités sans que cette liste ne soit limitative.
157. La Région n'est pas responsable des dommages de toute nature qui peuvent résulter de ces changements ou opérations de maintenance et/ou d'une indisponibilité temporaire.
158. La Région se réserve le droit de compléter ou de modifier, à tout moment, les services numériques et outils informatiques en fonction de l'évolution des technologies.

15. Contrôle et audit

159. Les opérations de contrôle et d'audit se distinguent des opérations de maintenance car elles visent à vérifier que l'utilisation des outils, services et locaux mis à disposition s'effectue dans un cadre scolaire, à des fins éducatives et pédagogiques et est bien licite.
160. Elles se justifient par les obligations incombant à la Région.
161. En effet, de par ses missions, la Région est soumise à une obligation générale de sécurité.
162. A ce titre, l'utilisation des services numériques et outils informatiques pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, d'optimiser cette même utilisation ou encore de mener des analyses statistiques.
163. La Région se réserve ainsi le droit, notamment :
 - de vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;
 - de diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées sur les ressources du système d'information ;
 - de contrôler l'origine licite des logiciels installés ;
 - de conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information ;

- de transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

164. En outre, en cas d'incident, la Région se réserve le droit de :

- surveiller le contenu des informations qui transitent sur son système d'information ;
- vérifier le contenu des disques durs des ressources du système d'information attribuées aux utilisateurs ;
- vérifier les contenus et messages en cas de soupçon de contenu illicite ;
- supprimer les éventuels contenus illicites identifiés du système d'information ;
- procéder à toutes copies utiles pour faire valoir ses droits.

16. Responsabilité et sanctions

165. L'utilisateur est responsable de toute utilisation non conforme aux conditions et limites définies par cette charte, notamment des actes de téléchargement d'œuvres protégées sans autorisation.
166. L'utilisateur est seul responsable de l'utilisation des services numériques et outils informatiques et des dommages directs et indirects, matériels ou immatériels, qui pourraient en résulter.
167. La Région n'exerce aucun contrôle sur les contenus publiés, postés, transmis ou reçus par les utilisateurs quel que soit l'espace sur lequel ces contenus sont publiés, postés ou transmis.
168. Une protection contre les intrusions, virus ou toute manœuvre illicite ne peut être garantie. La Région décline toute responsabilité concernant de tels événements. De même, la Région ne peut garantir la confidentialité des données et de communications transmises par le réseau Wi-Fi/filaire mis à disposition des utilisateurs.
169. En outre, la responsabilité de la Région ne saurait être recherchée en cas d'usage frauduleux, illicite ou abusif ou dû à une divulgation volontaire ou involontaire à quiconque de son mot de passe.
170. L'utilisateur garantit la Région contre toute action qui serait engagée à son encontre, ou toute plainte qui serait déposée contre elle, par un tiers, du fait de l'utilisation des services numériques et outils informatiques de la Région.
171. En cas de faisceau d'indices laissant supposer qu'un utilisateur met en cause les intérêts et la sécurité de la Région, en ne respectant pas les règles instituées par cette charte, la Région se réserve le droit de contrôler les traces individuelles des connexions incriminées.
172. L'ensemble des traces, logs, données d'identification, données de trafic, données d'identification, sans que cette liste ne soit exhaustive, peut servir à titre d'élément de preuve.
173. En cas de non-respect avéré et suivant la gravité des faits, les droits d'accès de l'utilisateur concerné pourront être suspendus, temporairement ou définitivement.

174. Tous les matériels, les logiciels ou les applications installés illicitement seront supprimés ou désactivés par la Région dès le constat de leurs présences sur des postes de travail ou des matériels nomades, ou le simple constat de leurs accessibilités.
175. L'utilisateur est responsable de l'utilisation des systèmes d'information et de communication en conformité avec la présente charte.
176. Toute mauvaise utilisation ou utilisation non conforme aux conditions et limites définies par cette charte est constitutive d'une faute.
177. En conséquence, le non-respect des dispositions légales et réglementaires, ainsi que de cette charte, expose l'utilisateur en cause à des sanctions disciplinaires, et/ou à des poursuites judiciaires.
178. La Région se réserve le droit d'agir en justice contre tout utilisateur ayant causé un préjudice de quelque nature que ce soit.
179. En outre, l'utilisateur s'expose à des sanctions concernant son droit d'utiliser les systèmes d'information et de communication, notamment, le contrôle renforcé, la suspension, le blocage, le retrait et même la suppression pure et simple de son droit d'utiliser tout ou partie des systèmes d'information et de communication, des sites web et des applications, ou l'exclusion.
180. La Région pour sa part, déclare mettre en œuvre, par le biais notamment de cette charte, tous les efforts nécessaires à un bon usage des systèmes d'information et de communication et n'assumer aucune responsabilité au titre des agissements fautifs ou délictueux des utilisateurs auxquels elle fournit un droit d'accès.

Annexe : Fiche pédagogique relative à la protection des données personnelles des élèves

Cette fiche pédagogique a pour objectif de vous expliquer comment nous faisons pour protéger vos données personnelles.

Les données personnelles, de quoi s'agit-il ?

Les données personnelles sont des informations qui permettent de savoir qui vous êtes et de vous identifier.

Ce sont les données qui se rattachent directement ou indirectement à vous en tant que personne.

Lorsque vous communiquez ces données à quelqu'un, celles-ci permettent à cette personne de savoir qui vous êtes.



Les données à caractère sensible

Il existe une catégorie de données personnelles auxquelles il faut porter une attention particulière car elles sont très personnelles et donc **sensibles**.



Il est en principe interdit d'avoir des données sensibles sur quelqu'un sauf cas exceptionnels.

Parfois, il est possible que votre établissement soit autorisé à avoir ce type d'information. C'est par exemple le cas si vous avez une maladie qui nécessite un traitement spécifique quand vous êtes dans votre établissement scolaire. Dans un tel cas, des mesures particulières sont prises par votre établissement pour protéger vos données personnelles.

Sachez que la Région Ile-de-France ne collecte pas d'information de ce type vous concernant.

Collecte de vos données personnelles

Quotidiennement, vos données personnelles sont collectées et traitées.

Par exemple :

- Lorsque vous vous connectez à votre compte ENT avec votre login ;
- Lorsque votre enseignant vous envoie des devoirs à faire sur votre adresse email ;
- Lorsque vous vous connectez avec vos identifiants sur les réseaux sociaux tels que Instagram, Tik Tok, Facebook, etc. ;
- Lorsque vous faites une commande sur internet et que vous payez avec une carte de crédit ou que vous vous inscrivez avec votre adresse email à une newsletter ;
- Lorsque vous créez un compte email sur une plateforme telle que Google.

La collecte de vos données personnelles est souvent nécessaire à la personne qui les demande pour pouvoir, par exemple, gérer votre compte ENT, vous identifier sur les réseaux sociaux ou encore vous permettre d'acheter sur un site internet, etc.

Il existe des lois qui veillent à ce que vos données personnelles soient protégées et qui vous donnent des droits sur vos données personnelles. En France et dans toute l'Europe, le **Règlement Général sur la Protection de Données Personnelles (« RGPD »)** s'applique.

Il est très important que vous compreniez que vous ne devez pas communiquer à n'importe qui vos données personnelles.

Vous ne devez pas communiquer n'importe quelles données, **uniquement les données personnelles qui sont nécessaires.**


Les règles de base à respecter par une personne qui traite vos données personnelles

Voici quelques règles que vous devez savoir lorsque vous communiquez vos données personnelles :

- La collecte de vos données personnelles doit avoir un **fondement**. Par exemple, vous avez donné votre accord ou encore la personne qui collecte vos données est obligée de le faire parce que la loi lui impose.
- La personne qui vous demande vos données doit vous **expliquer de façon claire** pourquoi elle a besoin de vos données. Par exemple, suite à votre achat en ligne, le vendeur a besoin de vos nom, prénom et adresse postale pour vous livrer votre commande.
- La personne qui vous demande vos données personnelles doit vous dire **pendant combien de temps** elle va les conserver ;
- **La collecte de vos données personnelles** doit être réalisée « **a minima** », c'est-à-dire que seules vos données personnelles strictement nécessaires doivent être communiquées ;
- La personne qui collecte vos données personnelles doit vous dire **les droits que vous avez sur vos données personnelles** et comment faire si vous souhaitez exercer vos droits. Vous avez par exemple le droit d'y accéder, de les corriger ou, dans certains cas, de demander leur suppression.

17. Connexion via un compte Google

 **La création d'un compte Google n'est pas nécessaire pour utiliser votre tablette ni pour accéder aux applications pédagogiques. Vous n'avez donc pas à vous connecter ou à créer de compte Google. Il vous suffit de fermer la fenêtre pop-up vous proposant la création ou la connexion à un compte Google.**

 **Si vous décidez de créer un compte Google, vos données personnelles seront recueillies directement par la société Google. Pour maîtriser et comprendre ce qu'il sera fait de vos données, lisez attentivement la politique de confidentialité de Google accessible à l'adresse suivante : <https://policies.google.com/privacy?hl=fr> qui vous explique comment sont utilisées vos données personnelles.**

 **En cas de connexion ou de création à un compte Google, certaines de vos données personnelles sont susceptibles d'être transférées en dehors de l'Union européenne, en particulier vers les Etats-Unis.**

Vous souhaitez en savoir plus sur les traitements de vos données personnelles par la Région ?

N'hésitez pas à consulter la charte sur la protection des données personnelles des élèves, personnels enseignants et non enseignants.

Vous avez une question ?

Notre équipe est disponible pour vous aider !

Notre Délégué à la protection des données est votre point de contact pour toute question relative à la manière dont nous traitons vos données personnelles.

N'hésitez pas à le contacter pour toute question :

- son adresse de courrier électronique est : dpo@iledefrance.fr
- son adresse postale est : Région Ile-de-France, Pôle Juridique Achats Données, à l'attention du Délégué à la Protection des Données, 2 rue Simone Veil, 93400 Saint Ouen.