CHARTE INFORMATIQUE
RELATIVE A L'UTILISATION DES MOYENS INFORMATIQUES ET DE COMMUNICATION ELECTRONIQUE

13 juin 2016

Sommaire analytique

Article 1. **Préambule**

1. Le Centre national de la fonction publique territoriale (ci-après, le CNFPT) est un établissement public administratif, unique, paritaire et déconcentré regroupant les collectivités territoriales et leurs établissements, au service de ceux-ci et de leurs agents[1].

2. En raison de l'importance centrale que prend l'outil informatique dans le travail quotidien de son personnel, le CNFPT a décidé de se doter de la présente charte qui a pour objet de fixer les règles d'utilisation des moyens informatiques et de communication électronique au sein de l'établissement.

3. Les règles ainsi définies sont destinées à assurer un usage des moyens informatiques et de communication électronique conforme à leur objet, ainsi qu'aux dispositions légales et réglementaires applicables.

4. La présente charte tient compte notamment des recommandations de la Commission nationale de l'informatique et des libertés (Cnil)[2] ou celle de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

5. La présente charte, s'inscrit également dans le cadre de la loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires qui fixe un certain nombre d'obligations applicables au domaine de l'informatique et des communications électroniques telles que le secret professionnel, la discrétion ou la dignité.

6. La présente charte est rédigée dans le souci de concilier les intérêts et obligations de chaque utilisateur et ceux du CNFPT. Elle manifeste ainsi la volonté du CNFPT d'assurer un usage loyal, respectueux et responsable de ses moyens informatiques et de communication électronique, ainsi que de protéger son patrimoine et son image de marque.

7. La présente charte n'a pas pour objet et objectif de couvrir de façon exhaustive tous les cas de figure susceptibles de se présenter dans le cadre de l'utilisation des moyens informatiques et de communication électronique mis à la disposition des utilisateurs. C'est dans l'esprit des règles ainsi édictées et des droits et devoirs généraux des agents publics que chacun devra se conformer dans des situations non envisagées.

8. La présente charte pourra évoluer en fonction du contexte légal et, le cas échéant, de la politique de sécurité notamment applicable au sein du CNFPT.

9. Ces règles ont également pour objet d'atteindre un niveau optimum en termes de sécurité, de confidentialité et de performance dans l'usage de ces moyens.

10. La présente charte est publiée sur l'intranet et les agents sont formés pour l'application des règles d'utilisation prévues par la présente charte.

Article 2. **Portée et opposabilité**

11. Le présent document se présente sous la forme d'un acte réglementaire (dénommé « charte »), édicté après avis du comité technique, qui s'impose à ses destinataires sans

[1] article 12 de la loi n° 84-53 du 26 janvier 1984

[2] Voir notamment Fiche n° 7 du rapport pour les employeurs et les salariés, 2008, de la Cnil.

nécessité de consentement. La charte pose des règles générales, impersonnelles et impératives. Les manquements à cette charte sont sanctionnés sur le terrain de la responsabilité disciplinaire, sans préjudice de possibles recours sur le plan civil ou pénal.

12. Dès lors que la charte est publiée (notamment sur le site intranet du CNFPT, accessible à tous les utilisateurs), elle est exécutoire.

13. En conséquence, l'utilisateur est réputé en avoir pris connaissance.

Article 3. Champ d'application

3.1 Personnes concernées

14. La présente charte est applicable à toute personne autorisée à accéder aux moyens informatiques et de communication électronique, ce quel que soit leur statut (agents de la fonction publique titulaires et contractuels, vacataires, élèves, etc.). Ces personnes sont désignées dans la présente charte par le terme « utilisateurs ».

15. Toutefois, la présente charte peut être complétée de documents spécifiques pour certaines catégories de personnel.

3.2 Moyens concernés

16. Sont visés par la présente charte :

- l'ensemble des moyens informatiques et de communication électronique qui sont la propriété du CNFPT et/ou qui sont mis par lui à la disposition des utilisateurs à des fins professionnelles ou plus généralement dans le cadre de ses missions ;

- l'ensemble des moyens informatiques et de communication électronique qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu une autorisation d'utilisation dans le cadre de son activité professionnelle ou des missions du CNFPT.

3.3 Usages concernés

17. La présente charte s'applique à tous les types d'usage qu'ils aient lieu :

- dans les locaux du CNFPT ;

- dans les locaux dans lesquels le CNFPT exerce ses missions ;

- 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.

18. La présente charte s'applique quelles que soient la fréquence et la périodicité de l'utilisation des moyens informatiques et de communication électronique.

Article 4. **Conditions d'utilisation**

4.1 Usage professionnel

19. Les moyens informatiques et de communication électronique sont réservés à un usage professionnel.

20. En particulier, l'adresse électronique est strictement professionnelle. Elle ne doit donc pas être utilisée dans un autre contexte, et notamment diffusée sur des sites internet (chats, forums, blogs, etc.), sans rapport avec l'activité professionnelle.

21. L'inscription sur des listes de diffusion permettant la réception automatique et périodique d'informations est également réservée à un usage professionnel.

22. Elle est basée sur un principe d'autodiscipline des utilisateurs, destiné à s'assurer d'une part, de la pertinence et de la nécessité d'une telle inscription et d'autre part, des conséquences de celle-ci (fréquence de réception des messages, poids des messages, encombrement des réseaux, etc.).

23. L'accès à des services en ligne (sites web, blogs, forums, chats, etc.) est également réservé à un usage professionnel.

24. Dans tous les cas, et quelles que soient les conditions effectives d'utilisation, l'usage des moyens informatiques et de communication électronique est présumé avoir un caractère professionnel.

25. Sont ainsi présumés avoir un caractère professionnel, notamment :

- les fichiers créés grâce à ces moyens par un utilisateur, pour l'exécution de son travail, sauf lorsque celui-ci les identifie comme étant personnels ;

- les connexions établies par un utilisateur sur des sites internet pendant son temps de travail grâce à un moyen informatique ou de communication électronique, pour l'exécution de son travail.

26. Il en résulte que le CNFPT peut y accéder hors de la présence de l'utilisateur.

4.2 Usage non professionnel

27. Bien que les moyens informatiques et de communication électronique soient réservés à un usage professionnel, leur utilisation à des fins non professionnelles, pour répondre à des obligations socialement admises, est tolérée.

28. L'usage des moyens informatiques et de communication électronique se traduit dans les faits par :

- la possibilité de créer un répertoire informatique non professionnel ;

- la possibilité d'utiliser l'adresse électronique à des fins non professionnelles.

29. Cette tolérance s'inscrit dans le strict respect des règles ci-après :

- cet usage doit donc être mesuré et demeurer raisonnable ;

– un tel usage ne doit pas :

  - perturber le bon fonctionnement des moyens informatiques et de communication électronique, du service et du CNFPT en général ;

  - compromettre ses activités et particulièrement ses missions d'intérêt général et la continuité du service ;

  - porter atteinte aux obligations qui incombent aux agents et notamment les obligations de dignité, de loyauté, de discrétion, de neutralité ou de réserve ;

  - ne doit en aucun cas porter sur des contenus illégaux ou illicites, ou à caractère pornographique, xénophobes, racistes ou antisémite, ou violents, ou d'incitation à la violence ou à la haine raciale, ou d'incitation à la commission d'actes illicites, ou encore des sites de rencontres, de jeux en ligne,etc.

  - ne doit en aucun cas porter atteinte ou être susceptible d'engager la responsabilité du CNFPT ;

  - poursuivre un but lucratif ou ludique.

30. La confidentialité attachée au répertoire informatique non professionnel est conditionnée par le fait que ce répertoire soit clairement identifiable en tant que tel.

31. Le répertoire informatique privé, utilisé pour stocker des documents personnels, doit être identifié par le terme : « privé » ou « prive ». Le répertoire informatique privé ne doit en aucun cas être stocké sur les répertoires partagés sur le réseau ou sur le répertoire de sauvegarde.

32. Tous les répertoires informatiques ne portant pas cette mention, sont considérés comme « professionnels ».

33. Ce stockage doit, de la même manière que pour tout usage non professionnel des moyens informatiques et de communication électronique mis à disposition par le CNFPT, répondre à des obligations socialement admises. Il doit donc demeurer raisonnable. Les dites obligations disparues, les répertoires informatiques identifiés comme étant privés doivent être supprimés ou transférés sur tous moyens personnels par l'utilisateur concerné.

34. Il est rappelé que l'adresse électronique professionnelle prenom.nom@cnfpt.fr mise à disposition de l'utilisateur par le CNFPT est réservée à un usage professionnel.

35. Néanmoins pour répondre à des besoins socialement admis, l'utilisateur peut émettre ou recevoir des courriers électroniques non professionnels sur son adresse électronique professionnelle, la confidentialité attachée à la correspondance privée implique la notion du terme « privé » ou « prive » dans la zone « objet du message ». La perspective d'une réponse impose d'informer le tiers destinataire du message de cet usage. Ces messages peuvent être archivés dans un dossier spécifique de la boite de réception de l'utilisateur. Ce dossier spécifique doit être identifié par le terme : « privé » ou « prive ».

36. Tout courrier électronique envoyé ou reçu à partir de l'adresse électronique professionnelle prenom.nom@cnfpt.fr ne portant pas la mention « privé » ou « prive » dans la zone « objet du message », ou enregistré ailleurs que dans le dossier « privé » ou « prive » est considéré comme professionnel.

37. Lorsque le moyen de communication utilisé ne comporte pas de champ « objet » (chat, messagerie instantanée,..), le message à caractère personnel doit débuter par le terme « privé » ou « prive ».

38. Aucune information à caractère professionnel ne doit être ni stockée dans le répertoire informatique « privé » ou « prive », ni émise ou reçue via courrier électronique identifié comme « privé » ou « prive ».

39. L'usage des moyens informatiques et de communication électronique à des fins non professionnelles étant une tolérance et non un droit, le CNFPT se réserve le droit de limiter ou de suspendre cette tolérance en cas d'abus, notamment d'usage excessif par sa durée sur le temps de travail.

40. L'usage des moyens informatiques et de communication électronique à des fins non professionnelles relève de la seule et entière responsabilité de l'utilisateur, qui dégage en conséquence le CNFPT de toute responsabilité.

41. Le caractère non professionnel de l'usage des moyens informatiques et de communication électronique interdit, par principe, au CNFPT d'accéder aux contenus ou données émis, reçus ou échangés dans ce cadre.

42. Le caractère « non professionnel » du répertoire ou des courriers électroniques échangés, ne fait pas obstacle à ce que :

- le CNFPT puisse accéder de manière exceptionnelle à ces éléments lorsqu'il existe un risque avéré pour le CNFPT en termes notamment de sécurité, de continuité de service, ou un risque grave de voir sa responsabilité engagée ;

- ces éléments fassent l'objet de conservation technique dans le cadre des procédures de sauvegarde (« back up ») ou de plans de continuité ou reprise d'activité mises en œuvre au sein du CNFPT ;

- en cas de détection ou de suspicion de la présence d'un code malveillant, à la mise en quarantaine ou le cas échéant, à la suppression de l'élément quelconque qui comporte ou comporterait un code malveillant ;

- un administrateur ou toute personne habilitée, accède à ces contenus dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des moyens informatiques et de communication électronique, ce notamment dans le cadre d'opération de maintenance ;

- le CNFPT puisse, dans tous les autres cas, et pour des motifs légitimes, accéder à ces éléments en présence de l'utilisateur ou ce dernier dûment appelé, ou, en son absence, dès lors qu'il y est autorisée par une décision de justice ou une autorité habilitée à cet effet (police, gendarmerie, douanes, Cnil, contrôle tutélaire, contrôle réglementé [ex : Cour des comptes], etc.).

43. L'utilisateur concerné est informé préalablement à tout accès aux données ou contenus identifiés comme privés. Si cette information préalable est impossible, elle est remplacée par une information a posteriori. Les personnes habilitées à ces opérations veillent à respecter la confidentialité de ces informations.

Article 5. **Conditions d'accès et d'identification**

44. Chaque utilisateur est doté d'un ou de plusieurs identifiants permettant l'accès aux moyens informatiques et de communication électronique.

45. L'identifiant peut prendre diverses formes (login/password, signature électronique, cartes avec ou sans contact, etc.).

46. L'identifiant est dans tous les cas personnel et confidentiel.

47. Il est dès lors interdit à l'utilisateur :

- de procéder à la moindre divulgation, même intra-service, de son ou de ses identifiant(s) ;
- d'utiliser un identifiant autre que le sien, dans l'hypothèse où il en aurait eu connaissance ;
- de supprimer, masquer ou modifier son identité ou son identifiant ;
- d'user de son droit d'accès pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu l'autorisation d'accès.

48. Si ces identifiants, par nature confidentiels, ont fait l'objet d'une communication ou qu'il existe un risque qu'ils aient été communiqués, ou encore s'ils ont été oubliés, l'utilisateur concerné doit, selon la procédure mise en place par le CNFPT, renouveler ses identifiants. S'il existe une difficulté à ce renouvellement, ce dernier doit se rapprocher de la direction des systèmes d'information et des télécommunications.

49. L'identifiant doit être modifié selon une fréquence déterminée par la direction des systèmes d'information et des télécommunications ou selon la politique de sécurité mise en place par du CNFPT.

50. Lorsqu'un accès à distance est accordé à un utilisateur, celui-ci s'engage à utiliser, à l'exclusion de tout autre, les moyens techniques d'authentification qui lui seront remis.

51. En termes de sécurité et de confidentialité, l'utilisateur est soumis aux mêmes obligations que celles visées pour la gestion des identifiants et devra suivre toutes les prescriptions complémentaires qui lui seront signifiées.

52. Il devra aviser, sans délai, les services compétents de la perte ou du vol des moyens d'authentification à distance. Il devra également, selon les cas, soit assister le CNFPT, soit procéder lui-même à toutes les démarches (déclaration d'assurance, dépôt de plainte, etc.) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

53. La suppression et la suspension d'autorisation d'accès aux moyens informatiques et de communication électronique font l'objet d'une procédure formalisée destinée à dégager l'utilisateur de sa responsabilité.

54. Sauf à avoir engagé préalablement une demande de suspension ou de suppression d'autorisation, ou à être en mesure de démontrer le contraire, tout usage des moyens informatiques et de communication électronique est réputé avoir été réalisé par le bénéficiaire de l'identification d'accès qui en assume toutes conséquences, notamment juridiques et financières.

55. Le CNFPT se réserve, en cas de nécessité et notamment pour raison découlant de l'application de la présente charte, de manière temporaire ou définitive, le droit d'accorder, de refuser, de modifier ou de supprimer entièrement ou partiellement, le droit d'accès de toute personne aux moyens informatiques et de communication électronique.

56. Elle s'efforcera, autant que faire se peut, de prévenir l'utilisateur concerné dans des délais raisonnables, notamment en cas de maintenance.

Article 6. **Mobilité**

57. Dans le cadre de ses déplacements professionnels, quel que soit leur durée ou leur fréquence, l'utilisateur assure la garde et la responsabilité des moyens informatiques et de communication électronique qui lui ont été confiés.

58. Cet usage de moyens informatiques et de communication électronique dits « nomades » impose à l'utilisateur un niveau de surveillance et de confidentialité renforcé.

59. En particulier, l'utilisateur se doit d'adopter une attitude de prudence et de réserve au regard des informations et des ressources du système d'information du CNFPT qu'il pourrait être amené à manipuler ou à échanger.

60. Il doit également veiller à ce que des tiers non autorisés ne puissent accéder à ces moyens, les utiliser ou accéder à leurs contenus.

61. En cas non seulement d'incident avéré mais également de doute, l'utilisateur doit immédiatement en aviser le CNFPT.

Article 7. **Gestion des absences et des départs**

62. Chaque utilisateur doit veiller à ce que la continuité du service soit assurée, conformément aux modalités d'organisation définies par le CNFPT. Dans ce cadre, et dans une logique collaborative, il privilégie l'enregistrement de fichiers et de données sur des supports et emplacements accessibles à l'ensemble des personnes habilitées à y avoir accès plutôt que sur des supports et emplacements auquel il est seul à accéder.

63. En cas d'absence, il peut notamment recourir à l'utilisation d'automatisme de gestion de messagerie électronique (réponse automatique d'absence, transfert de messagerie).

64. En cas d'absence de l'utilisateur, pour quelque raison et durée que ce soit, le CNFPT se réserve le droit d'accéder directement aux différents dossiers, répertoires, courriers électroniques et plus généralement tous documents à caractère professionnel de l'utilisateur, ayant recours en tant que de besoin, aux codes administrateurs systèmes.

65. À l'annonce du départ d'un utilisateur du CNFPT, et pour des raisons légitimes de protection de ses intérêts, les droits d'accès et les conditions d'utilisation des moyens informatiques et de communication électronique pourront être modifiés. De même, des règles particulières de traçabilité pourront être mises en œuvre.

66. Lors de son départ, l'utilisateur doit remettre en bon état général de fonctionnement, l'ensemble des moyens informatiques et de communication électronique qui lui ont été remis.

67. Sauf nécessité liée à la continuité du service et pour un temps raisonnable qui ne saurait excéder trois mois, le compte messagerie de l'utilisateur est désactivé le jour de son départ.

68. Ses identifiants sont également désactivés.

69. Si l'utilisateur a bénéficié d'un moyen d'authentification à distance, il s'engage à le restituer.

70. Le répertoire identifié comme étant personnel, ainsi que tous les documents de même nature, doivent être supprimés par l'utilisateur au plus tard la veille de son départ du CNFPT.

71. À défaut, et sauf procédure judiciaire ou enquête administrative, ces éléments sont automatiquement supprimés le lendemain du départ de l'utilisateur du CNFPT, sans être consultés et sans qu'aucune copie n'en soit réalisée.

Article 8. Gestion des connaissances et de l'espace collaboratif

72. Le CNFPT privilégie, autant que faire se peut, le partage et la capitalisation des connaissances, et peut être ainsi amené à mettre en place des espaces collaboratifs de travail.

73. La qualité des informations ainsi disponibles est un objectif élevé et chaque utilisateur s'engage à être attentif à la pertinence des informations diffusées au sein de ces espaces et à travers les outils de gestion des connaissances mis à sa disposition.

74. Par souci de qualité, de responsabilité et de protection du patrimoine informationnel du CNFPT, l'utilisation de ces mêmes espaces et outils peut faire l'objet d'opérations de contrôle, d'audit, de modération et de traçabilité renforcées.

75. Aux mêmes fins, le CNFPT peut mettre en place des outils de marquage de tout ou partie des éléments des bases de données constituées dans ce cadre, pour éviter toute extraction. Les utilisateurs seront avertis de la présence de tels outils.

Article 9. Réseaux sociaux

76.L'utilisation des réseaux sociaux peut être source de risque et de responsabilité notamment en termes d'image. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées.

9.1 Usage professionnel

77. L'usage de réseaux sociaux professionnels peut être autorisé par le supérieur hiérarchique de l'utilisateur, seul compétent pour en déterminer les conditions d'utilisation.

78. De plus, si l'autorisation a été donnée, l'utilisateur devra :

- s'abstenir de publier un contenu de façon anonyme et, au contraire, s'identifier clairement, en précisant sa fonction au sein du CNFPT ;

- répondre aux contributions des tiers avec pertinence, exactitude, en s'efforçant de ne pas porter atteinte à l'image du CNFPT ;

- ne pas laisser à penser à ses interlocuteurs qu'il s'exprime au nom du CNFPT, sauf s'il y est habilité ;

- respecter les conditions générales d'utilisation du réseau social et l'ensemble des lois applicables (notamment en matière de concurrence, de consommation et de propriété intellectuelle) ;

- utiliser uniquement les outils de communication du CNFPT, selon les instructions qui lui ont été données et valoriser la visibilité du site web du CNFPT ;

- s'abstenir de diffuser toute information confidentielle ou toute information sensible relative au CNFPT. ;

79. En cas de doute sur l'utilisation d'un réseau social, l'utilisateur devra immédiatement consulter son supérieur hiérarchique.

80. L'autorisation donnée pourra être retirée, modifiée ou suspendue par le supérieur hiérarchique.

81. L'utilisateur devra prendre toutes les précautions utiles pour que son utilisation des réseaux sociaux soit sans danger pour les systèmes d'information du CNFPT.

9.2 Usage non professionnel

82. En dehors de la sphère professionnelle, et dès lors que les outils et moyens informatiques et de communication électronique confiés par le CNFPT à l'utilisateur ne sont pas utilisés, l'utilisateur est bien évidemment libre d'utiliser les réseaux sociaux. Cependant il s'interdit de porter atteinte à ses devoirs de neutralité et de discrétion professionnelle et de communiquer notamment des informations confidentielles, des informations sensibles relatives au CNFPT ou des informations couvertes par un secret légalement protégé, des informations relatives aux conditions de travail, à l'organisation générale, au calendrier d'évènements, à la rémunération, etc..

83. Les catégories proposant, à la fois, des contenus à caractère professionnel et personnel tels que les réseaux sociaux et les forums sont autorisés dans la limite d'un usage raisonnable et à condition de ne pas mettre en cause l'intérêt ou la réputation du CNFPT.

84. L'utilisateur n'est autorisé à faire mention de son appartenance au CNFPT que dans la mesure où cette divulgation ne porte pas atteinte à ses obligations de discrétion et de neutralité, ni à l'image ou à la réputation du CNFPT.

9.3 Signalement

85. Qu'il utilise les réseaux sociaux à titre professionnel ou non professionnel, l'utilisateur pourra informer le CNFPT d'un agissement de tiers dont il aurait connaissance susceptible de porter atteinte à la réputation de l'établissement ou à l'un de ses droits (notamment de propriété intellectuelle).

Article 10. Utilisation professionnelle de matériel personnel

86. L'usage de matériels informatiques ou de communication personnels, à titre professionnel n'est pas autorisé sur le réseau interne du CNFPT, en raison notamment des problématiques importantes de sécurité et de confidentialité des données professionnelles.

87. La connexion de matériels informatiques ou de communication personnels au réseau interne du CNFPT n'est pas autorisée, sauf autorisation écrite de la direction des systèmes d'information et des télécommunications et sous réserve de l'application stricte des consignes de sécurité transmises à l'utilisateur.

Article 11. Télétravail

88. Sont concernés par les dispositions de cet article uniquement les utilisateurs bénéficiant de la possibilité d'accomplir leur travail en télétravail et qui à ce titre ont déposés une demande auprès de leur supérieur hiérarchique du CNFPT, demande validée par le directeur de structure, le directeur général adjoint ou le directeur rattaché directement au directeur général pour les directions du siège et la direction générale adjointe chargée des ressources humaines et du dialogue social.

89. La mise en œuvre technique d'une solution de télétravail est conditionnée par l'édiction d'un arrêté ou d'un avenant au contrat qui précise les conditions du télétravail envisagé.

11.1 Règles d'utilisation des systèmes d'information dans le cadre du télétravail

90. Lorsque les utilisateurs ont été autorisés à accomplir leurs tâches en télétravail, ils doivent respecter les règles suivantes :

- respecter le paramétrage et la configuration des moyens informatiques et de communication électronique mis à disposition par le CNFPT,
- mettre en œuvre les procédures de mise à jour demandées des moyens informatiques et de communication par le CNFPT et ce dans un délai de 48 heures et selon la procédure transmise à l'utilisateur,
- ne pas s'opposer aux moyens de traçabilité mis en place sur les moyens informatiques et de communication électronique mis à disposition par le CNFPT,
- respecter les systèmes de protection des données mis en place par le CNFPT sur les moyens informatiques et de communication électronique,

- veiller à utiliser tous les moyens de sécurité et de protection mis à disposition par le CNFPT afin de protéger les moyens informatiques et de communication électronique,

- respecter les restrictions à l'usage des moyens informatiques et de communication électronique mis en place par le CNFPT,

- prévenir sans délai le service dédié du CNFPT en cas d'incidents et ce conformément à la procédure transmise à l'utilisateur,

- en cas de panne ou de dysfonctionnement des moyens informatiques ou de communication électronique empêchant notamment le bon accomplissement des tâches, prévenir sans délai le service technique dédié du CNFPT et ce conformément à la procédure transmise à l'utilisateur,

- respecter les normes de sécurité et d'hygiène en vigueur pour les installations électriques et le lieu d'exécution du télétravail et ce afin de protéger les moyens informatiques et de communication électronique mis à disposition par le CNFPT,

- ne pas s'opposer à l'audit qui pourrait être mené par le CNFPT et qui pourra s'effectuer à distance selon les modalités prévues par ailleurs et dont l'utilisateur sera informé mais également en se rendant sur le lieu de télétravail de l'utilisateur, avec son autorisation si ce lieu est son domicile,

- en cas de retour à un travail dans les locaux du CNFPT pour quelques motifs que ce soit, rendre les moyens informatiques et de communication électronique mis à disposition et ce selon la procédure transmise à l'utilisateur.

11.2 Non-respect des dispositions

91. En cas de non-respect de ces dispositions, le CNFPT se réserve le droit de :

- demander à l'utilisateur de se mettre en conformité dans un délai de 48 heures ;

- restreindre l'accès à certains moyens informatiques ou applications mises à disposition par le CNFPT pour une période déterminée ou indéterminée.

Article 12. **Protection de la propriété intellectuelle**

92. L'utilisation des moyens informatiques et de communication électronique du CNFPT implique le respect des droits de propriété intellectuelle.

93. Sans que cette liste soit exhaustive, l'utilisateur s'engage à :

- utiliser les logiciels, applications, dans les conditions de la licence souscrite par le CNFPT ;

- ne pas effectuer de copie illicite de logiciel, d'applications et, a fortiori, de tenter d'installer des logiciels pour lesquels le CNFPT ne possèderait pas un droit d'usage ;

- ne pas reproduire et utiliser les bases de données, pages web ou autres créations du CNFPT 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 ni télécharger, ni même visualiser, des textes, des images, des photographies, des œuvres musicales ou audiovisuelles et, plus généralement, toute création copiée sur le réseau internet en violation des droits de propriété intellectuelle ;

- ne pas copier et remettre à des tiers des créations appartenant à des tiers ou au CNFPT sans s'assurer de l'autorisation du titulaire des droits qui s'y rapporte.

94. Le CNFPT respecte les droits de propriété intellectuelle des utilisateurs, dans le cadre de la législation en vigueur.

Article 13. **Préservation du secret et de la confidentialité**

95. Le respect de la confidentialité des données est une exigence essentielle du CNFPT.

96. La sauvegarde des intérêts du CNFPT nécessite le respect par l'utilisateur d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des informations dont il a connaissance dans le cadre de l'exercice de son activité professionnelle.

97. Le respect de cette obligation implique notamment de :

- veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations ;

- n'accéder qu'aux informations en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations réservées à d'autres utilisateurs ;

- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et le devoir de discrétion.

98. L'attention de l'utilisateur est attirée sur les risques liés à la diffusion de contenus d'information sur internet, en particulier au sein des réseaux sociaux et sur les blogs.

99. Il est donc strictement interdit de diffuser sur internet la moindre information à caractère professionnel, qu'elle soit ou non protégée par une obligation légale de secret ou une obligation contractuelle de confidentialité.

100. La diffusion de toute donnée ne peut être réalisée qu'aux conditions suivantes :

- habilitation de l'émetteur ;

- désignation d'un destinataire autorisé ;

- utilisation des moyens du CNFPT selon toutes les précautions de sécurité.

101. L'utilisation de procédés de cryptage est une fonction qui ne peut être mise en œuvre que dans certains cas autorisés, selon la procédure mise en œuvre par la direction des systèmes d'information.

Article 14. **Protection des données à caractère personnel**

14.1 Devoirs des utilisateurs

102. Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel. Ces dispositions figurent pour l'essentiel dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés ».

103. Dans ce cadre, en cas de mise en œuvre d'un traitement de données à caractère personnel, les utilisateurs devront avoir préalablement saisi le correspondant informatique et libertés du CNFPT à l'adresse cil@cnfpt.fr afin que celui en contrôle la conformité et se charge des formalités auprès de la Cnil.

104. Toute constitution de fichiers ou de bases de données comprenant des données à caractère personnel doit faire l'objet de formalités préalables auprès de la Cnil, sauf dérogations légales ou réglementaires. Dans ce cadre, l'utilisateur doit respecter les finalités des traitements de données à caractère personnel objets de ces formalités préalables.

105. Conformément à la loi « Informatique et libertés », les principes directeurs à respecter dans le cadre de la mise en œuvre d'un tel traitement sont les suivants :

- la pertinence et l'exactitude des données au regard des finalités poursuivies ;
- le consentement individuel à la collecte des données ;
- l'information des personnes concernées ;
- le droit d'accès, de rectification et d'opposition ;
- la protection adaptée aux risques présentés par le traitement sur les plans techniques et organisationnels.

106. La diffusion de données à caractère personnel à l'attention de tiers extérieurs à le CNFPT doit être rigoureusement contrôlée.

14.2 Droits des utilisateurs

107. Le CNFPT met en œuvre des traitements de données à caractère personnel concernant les utilisateurs. Le CNFPT s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale et licite, dans les conditions exposées. Ces données sont destinées aux personnes habilitées au sein du CNFPT ainsi qu'aux autorités habilitées.

108. Les traitements opérés dans le cadre de la présente charte ont pour finalité :

- le suivi et la maintenance des moyens informatiques et de communication électronique, qu'il s'agisse des applications informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;

- la gestion des annuaires permettant de définir les autorisations d'accès aux applications et réseaux ;

- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des moyens informatiques et de communication électronique, notamment la conservation des logs de connexion et des données de toute nature ;

- la gestion de la messagerie électronique ;

- le fonctionnement en réseaux internes par métiers ou par projet permettant la collecte, la diffusion ou la traçabilité de données de gestion des tâches, de la documentation, de la gestion administrative et des agendas des personnes répertoriées dans ces réseaux ;

- le respect de la présente charte.

109. À toutes fins utiles, il est rappelé que les données collectées auprès des utilisateurs sont nécessaires aux fins de bonne gestion et d'organisation des moyens informatiques et de communication électronique.

110. Conformément à la loi « Informatique et libertés », les utilisateurs sont informés, en particulier, qu'ils disposent d'un droit d'interrogation, d'accès, de rectification et d'opposition pour motif légitime au traitement des données les concernant et qui s'exerce auprès du Correspondant informatique et libertés du CNFPT.

Article 15. **Enregistrements**

15.1 Vidéo-protection

111. Le cas échéant, les utilisateurs accédant aux locaux du CNFPT sont informés de la mise en place d'un dispositif de vidéosurveillance à des fins de sécurité et de prévention des atteintes aux biens et/ou aux personnes.

112. L'enlèvement ou la neutralisation des caméras de surveillance sans justificatif est strictement interdit.

15.2 Enregistrements sonores/visuels

113. Dans le cadre professionnel et/ou dans l'objectif d'atteindre une certaine qualité de service, des outils techniques d'enregistrements sonores et visuels sont mis en place afin d'enregistrer les réunions professionnelles à distance. Sont concernées les conférences en ligne (webinaires). Ne sont pas concernés les appels téléphoniques (y compris les appels simultanés à plus d'une personne) et les visio-conférences.

114. Les utilisateurs sont informés de l'existence de ces outils d'enregistrement et du fait qu'ils sont activés par défaut sans qu'il soit besoin de le rappeler systématiquement à l'utilisateur.

115. Le CNFPT sollicitera l'autorisation des personnes concernées préalablement à toute exploitation des enregistrements visuels et sonores.

Article 16. **Sécurité**

116. Les moyens informatiques et de communication électronique sont exclusivement installés, configurés et paramétrés par le personnel habilité par le CNFPT.

117. Lorsqu'il s'agit de moyens personnels à l'utilisateur, ceux-ci sont nécessairement autorisés voire contrôlés par ce même personnel.

118. À des fins de précaution, certaines configurations peuvent être verrouillées par le CNFPT (poste de travail, accès internet, etc.).

119. La mise en place d'outils de sécurité par le CNFPT ne doit pas, toutefois, dispenser les utilisateurs d'une obligation de vigilance à cet égard.

120. En effet, tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens informatiques et de communication électronique mis à sa disposition, principalement en évitant l'introduction de codes malveillants susceptibles d'endommager le système d'information du CNFPT.

121. Cette vigilance passe notamment par le respect des règles de conduite suivantes :

- ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ou douteux ;
- ne pas faire suivre et détruire les messages du type « chaîne de solidarité » ;
- ne pas stocker et faire suivre des fichiers reçus ou trouvés sur internet ;
- ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir la direction des systèmes d'information et des télécommunications.

122. En cas de réception de messages non sollicités (« spams » ou pourriels) en dehors de sa boîte « courriers indésirables », l'utilisateur veille à :

- ne pas l'ouvrir ;
- ne pas y répondre ;
- ne pas le transférer.

123. L'utilisateur s'interdit également de :

- modifier les moyens mis à sa disposition notamment par l'ajout de logiciels, progiciels, même gratuits, ou de matériels pour quelque raison que ce soit ; si ces logiciels ou matériels lui semblent nécessaires pour l'exercice de sa mission, il en fait part à la direction des systèmes d'information et des télécommunications ;
- 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 du CNFPT.

124. D'une manière générale, toute installation ou utilisation de matériels non expressément autorisée par la direction des systèmes d'information et des télécommunications est interdite.

125. L'utilisateur est tenu d'informer, sans délai le CNFPT de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les moyens informatiques et de communication électronique. Il est tenu, en particulier, de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus à la direction des systèmes d'information et des télécommunications.

Article 17. **Traçabilité**

126. Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité à apporter la preuve, le cas échéant, du bon usage des moyens informatiques et de communication électronique mis à la disposition des utilisateurs, le CNFPT se réserve le droit de mettre en œuvre des outils de traçabilité tels que des journaux de connexions de l'ensemble des moyens informatiques et de communication électronique.

127. Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

Article 18. **Filtrage**

128. Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité de tenter de prévenir tout usage illicite de ces mêmes moyen, le CNPFT procède à la mise en place d'outils de filtrage (filtrage des contenus, des URL, protocolaire, etc.) permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre certaines catégories de sites internet.

129. Il est précisé que ces outils, en ce qu'ils portent entre autre sur l'accès à internet, permettent un contrôle des connexions des utilisateurs.

130. Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit. Un utilisateur constatant qu'un contenu licite et utile fait l'objet d'un filtrage erroné en informe la direction des systèmes d'information et des télécommunications pour demander la levée de ce filtrage.

Article 19. **Scan informatique**

131. La direction des systèmes d'information et des télécommunications met en œuvre des dispositifs de scans automatisés des postes de travail des utilisateurs à des fins de sécurité, de contrôle du respect des dispositions légales relatives à la propriété intellectuelle des logiciels et d'inventaire technique.

132. Deux types de scans sont mis en œuvre : d'une part le scan des postes de travail, des fichiers et des boites aux lettres de messagerie afin de détecter la présence éventuelle de virus ou de courrier indésirables, et d'autre part, le scan des postes des travail afin d'identifier les matériels et logiciels installés.

Article 20. **Mesures d'urgence et plan de continuité d'activité**

133. L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, le CNFPT peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la continuité de son activité et le respect de ses engagements contractuels ou légaux.

134. Dans cette hypothèse, l'utilisateur pourra être amené à la demande du CNFPT à prendre des mesures d'urgence et de sécurité spécifiques, qu'il applique sans délai.

135. Ces mesures exceptionnelles peuvent inclure, notamment, une dégradation de service sur tout ou partie des ressources du système d'information (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources du système d'information (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'information, télétravail, déplacement sur des sites de secours tiers, etc.).

Article 21. **Maintenance**

136. La mise à disposition des moyens informatiques et de communication électronique implique nécessairement des opérations de maintenance technique, qu'il s'agisse de maintenance corrective, de maintenance préventive ou de maintenance évolutive.

137. L'objectif de ces opérations n'est autre que d'assurer le bon fonctionnement et la sécurité des systèmes d'information. Elles se distinguent en cela des opérations de contrôle et d'audit mentionnées ci-après.

138. Ces opérations peuvent nécessiter l'intervention d'une « personne habilitée» soit sur site, soit à distance, conduisant alors cette personne à ce qui est couramment appelé « prendre la main à distance ». Cette intervention se fait dans la mesure du possible en présence de l'utilisateur, ou à tout le moins après qu'il en ait été informé.

139. En aucun cas, ces opérations, quel que soit leur mode opératoire, ne nécessitent que l'utilisateur communique son identification.

140. Dans ce cadre, la « personne habilitée» veille dans la mesure du possible à ne pas prendre connaissance des éléments privés présents sur le poste de l'utilisateur. S'il devait malgré tout y avoir accès, il veille à ne pas les conserver ni les divulguer.

141. Si, à l'occasion d'opérations de maintenance, une utilisation anormale et/ou un contenu illicite ou préjudiciable est identifié, le CNFPT en tirera toutes les conséquences.

Article 22. **Contrôle et audit**

142. Les opérations de contrôle et d'audit se distinguent des opérations de maintenance en ce qu'elles portent sur la régularité de l'utilisation des moyens informatiques et de communication électronique.

143. Elles se justifient par les obligations incombant au CNFPT et par un souci de sécurité et de bon fonctionnement des infrastructures du réseau informatique.

144. En effet, de par son activité, le CNFPT est soumis à une obligation générale de sécurité, en application des dispositions du Code pénal relatives à la protection des systèmes de traitement automatisés de données, et de la loi dite « Informatique et libertés ».

145. Le CNFPT dispose également, d'un pouvoir de contrôler l'activité des utilisateurs et en particulier, le respect par eux de la présente charte.

146. L'utilisation des moyens informatiques et de communication électronique pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, d'optimiser

l'utilisation conforme ou encore de mener des analyses statistiques. Les utilisateurs sont informés des mesures prises à cet effet.

147. Le CNFPT se réserve ainsi le droit, notamment de :

- vérifier le trafic informatique entrant et sortant, ainsi que le trafic transitant sur le réseau interne ;
- 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 ;
- contrôler l'origine licite des logiciels installés ;
- conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information ;
- transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

148. En outre, en cas d'incident, le CNFPT 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 ;
- procéder à toutes copies utiles pour faire valoir ses droits.

149. Ces opérations de contrôle et d'audit relèvent des missions de la direction des systèmes d'information et des télécommunications, qui a la charge de la qualité, de la protection et de la sécurité des moyens informatiques et de communication électronique fournis aux utilisateurs.

150. En particulier, dans le cadre de ses missions, elle exerce un contrôle notamment des durées de connexion et des sites les plus visités. En cas de perturbation induite par l'apparition intempestive d'alertes suite à des tentatives d'infection des systèmes à l'aide de virus informatiques, elle est habilitée à mener toutes les investigations qu'elle jugera utiles aux fins d'éradiquer lesdits virus.

151. Tout intervenant de la direction des systèmes d'information et des télécommunications doit impérativement respecter la confidentialité des échanges électroniques et des fichiers des utilisateurs.

152. Les utilisateurs sont toutefois informés que les administrateurs systèmes sont conduits, de par leurs fonctions, à avoir accès à l'ensemble des informations relatives aux utilisateurs (messages, connexions à internet, etc.), y compris à celles qui sont enregistrées sur le disque dur de leur poste de travail.

153. Néanmoins, ces administrateurs systèmes sont tenus au secret professionnel[3] et ne peuvent utiliser leurs droits d'administrateurs qu'à des fins strictement professionnelles.

[3] Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, article 26 et art. 226-13 c. pénal.

154. En cas de faisceau d'indices laissant supposer qu'un utilisateur met en cause les intérêts et la sécurité du CNFPT, en ne respectant pas les règles instituées par la présente charte, la direction des systèmes d'information et des télécommunications informe la direction générale, puis, sur sa demande écrite et motivée, transmet les traces individuelles des connexions incriminées.

155. En cas de non-respect avéré de la présente charte par un utilisateur, la direction des systèmes d'information et des télécommunications en avertit le supérieur hiérarchique de l'utilisateur pour que celui-ci décide de la suite à y donner.

156. En fonction des faits, les droits d'accès de l'utilisateur concerné pourront être suspendus temporairement ou définitivement, sans préjudice d'éventuelles sanctions disciplinaires.

157. Tout matériel installé illicitement sera supprimé ou désactivé par les intervenants de la direction des systèmes d'information et des télécommunications dès le constat de leur présence sur le poste de travail.

Article 23. **Consommations téléphoniques**

158. Pour la bonne gestion de ces ressources :

- pour les moyens informatiques et de communication électronique fixes, le suivi global des consommations est disponible via les opérateurs de téléphonie ;

- pour les moyens informatiques et de communication électronique nomades professionnels (téléphones portables, smartphones, tablettes, etc.), les informations individuelles de type date, heure, durée, coût et numéros appelés sont disponibles via les opérateurs téléphoniques mobiles, à travers les services de suivi des consommations qu'ils proposent.

159. Les informations ainsi disponibles, qui sont principalement dédiées à l'analyse des consommations, peuvent en tout état de cause être utilisées pour démontrer toutes utilisations contrevenantes aux termes de la présente charte ou pour servir de preuve d'un fait manifestement illicite.

Article 24. **Consommation de consommables**

160. Pour la bonne gestion de ses ressources, un suivi des consommables (ex : consommables d'impression, d'encre, papier, etc.) est mis en place par le CNFPT sur l'ensemble de ses équipements.

161. Dans le cas où une consommation anormale est détectée, le CNFPT se réserve la possibilité d'analyser l'origine de l'anomalie et les niveaux de consommation des utilisateurs concernés après qu'ils en aient été informés. Les restitutions ainsi obtenues sont nominatives et comprennent le détail des consommations (date, heure, nombre de feuilles, etc.).

162. Les informations ainsi disponibles, qui sont principalement dédiées à l'analyse des consommations, peuvent, en tout état de cause, être utilisées pour démontrer toutes utilisations contrevenantes aux termes de la présente charte ou pour servir de preuve d'un fait manifestement illicite.

Article 25. **Règles de conservation et de sauvegarde**

163. Chaque utilisateur doit mettre en œuvre et organiser, selon les instructions de sa hiérarchie, les moyens nécessaires à la conservation des messages et des informations de toute nature lorsque cela est nécessaire.

164. L'utilisateur est dans l'obligation, si elle existe, de respecter la politique de conservation et d'archivage mise en œuvre au sein du CNFPT, ainsi que les dispositions légales et réglementaires en vigueur.

165. Les traces détaillées d'activité sont conservées pendant les durées légales ou conventionnelles, à l'issue desquelles elles sont détruites.

166. Ces traces valent preuve de l'utilisation des moyens informatiques et de communication électronique.

167. Ces traces peuvent faire l'objet d'un traitement statistique.

168. Ces traces peuvent être fournies aux autorités compétentes selon les dispositions légales et réglementaires en vigueur.

169. Elles peuvent aussi être communiquées à l'utilisateur, pour les seules données qui le concernent directement et individuellement, en application des dispositions dites « données à caractère personnel ».

170. Les sauvegardes et back up réalisées par le CNFPT ne concernent pas les éléments du répertoire et les messages identifiés comme étant privés, qui sont donc conservés sous la seule et entière responsabilité de l'utilisateur.

Article 26. **Responsabilité et sanctions**

171. L'utilisateur est responsable :

- dans le cadre de son activité professionnelle, de l'utilisation des moyens informatiques et de communication électronique en conformité avec la présente charte ;

- dans la sphère de sa vie privée, de tout usage à caractère non professionnel des moyens informatiques et de communication électronique mis à sa disposition par le CNFPT, à l'exclusion de toute responsabilité de ce dernier.

172. Toute utilisation non conforme aux conditions et limites définies par cette charte peut être constitutive d'une faute.

173. En conséquence, le non-respect de la réglementation applicable expose l'utilisateur en cause à des sanctions disciplinaires, voire à des poursuites judiciaires.

174. En outre, des mesures visant à prévenir les atteintes ultérieures aux règles de la présente charte peuvent consister, notamment, dans le contrôle renforcé, la suspension, le blocage, le retrait et même la suppression pure et simple de son droit d'utiliser tout ou partie de ces moyens. Il peut, le cas échéant, être également exclu des espaces collaboratifs de travail.

175. Le CNFPT, pour sa part, déclare mettre en œuvre, par le biais notamment de la présente charte, tous les efforts nécessaires à un bon usage des moyens informatiques et de communication électronique et n'assumer aucune responsabilité au titre des agissements fautifs ou délictueux des utilisateurs auxquels elle fournit un droit d'accès.

176. L'utilisateur est informé que la multiplication de fautes dans l'utilisation des moyens informatiques et de communication électronique constitue une circonstance aggravante.

Article 27. **Dérogation**

177. Toute demande de dérogation aux termes de la présente charte doit être présentée, par écrit, au directeur général du CNFPT qui, après consultation du directeur des systèmes d'information et des télécommunications, se réserve le droit de l'accepter ou de la refuser.

Article 28. **Entrée en vigueur**

178. Le comité technique a examiné la présente charte et a donné un avis préalable à son application.

179. La présente charte entre en vigueur à compter du 1er juillet 2016.

LEXIQUE

Au sens de la présente charte, les termes ci-dessous ont la signification suivante :

- « accès distant » : il s'agit d'un accès à partir d'un site extérieur et quel que soit le lieu de cet accès (domicile, déplacement, etc.) aux moyens informatiques et de communication ;

- « espace collaboratif » : il s'agit d'un espace dédié à la collaboration entre différents utilisateurs ; il peut notamment prendre la forme d'un site internet, ou d'un serveur partagé. Cet espace a pour fonction de centraliser tous les outils liés à la conduite d'un projet, la gestion des connaissances ou au fonctionnement d'une organisation afin de les mettre à disposition des différents utilisateurs. L'objectif d'un espace collaboratif est de faciliter et d'optimiser la communication entre les différents utilisateurs d'un projet.

- « moyens de communication électronique » : moyens recouvrant internet et les télécommunications (équipement sans fil, carte de communication sans fil, téléphone, smartphone, terminaux portables, matériel nomade, messagerie électronique, forum, chat, visioconférence, etc.).

- « moyens informatiques » : moyens et ressources recouvrant tout matériel informatique (câblage, périphérique [tel qu'imprimantes simples ou multifonctions, webcam, etc...], disquette, CD-Rom, clé USB, ordinateur, tablette, PDA, photocopieurs, routeur, scanner, etc.) et toute ressource informatique de toute nature (telle que logiciels, applications, bases de données, etc.), et ce, qu'ils soient accessibles à distance, directement ou en cascade à partir d'un réseau.

- « matériel nomade » : moyens informatiques et de communication électronique portables, pouvant en conséquence être utilisés à l'extérieur des locaux du CNFPT.

- « donnée à caractère personnel » : toute information relative à une personne physique identifiée ou identifiable (personne concernée), directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

- « back up » : centre informatique externe possédant une configuration informatique compatible avec celle du CNFPT et prêt à accueillir les applications de cette dernière en cas de défaillance de son centre de traitement habituel.

- « code malveillant » : logiciel développé dans le but de nuire à un système informatique (virus, vers, chevaux de Troie, keylogger, etc.).