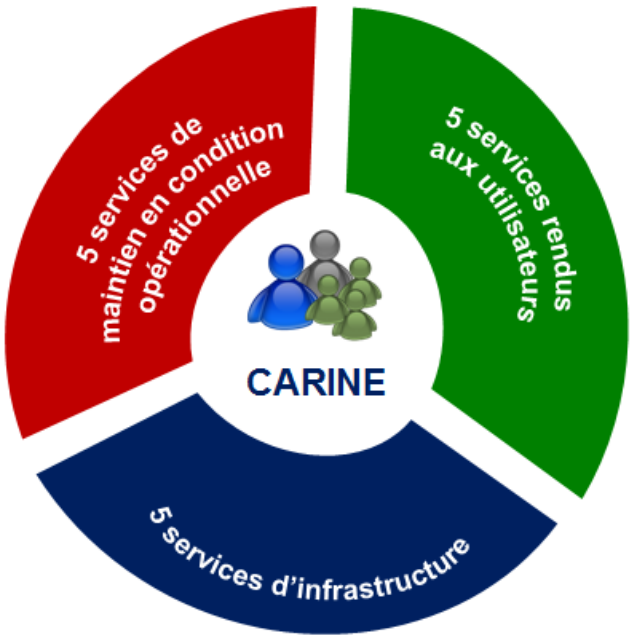
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉDUCATION
NATIONALE, DE
L'ENSEIGNEMENT
SUPÉRIEUR ET DE
LA RECHERCHE

L'école change avec le numérique
#EcoleNumerique

CARINE
CAdre de Référence des services d'Infrastructures numériques d'Établissements scolaires et d'écoles

version 1.0
juin 2016



http://eduscol.education.fr/CARINE

Sommaire

Préface

Le système éducatif s'est largement engagé ces dernières années dans la voie de l'appropriation des outils, des services et des ressources numériques. Des efforts importants ont été déployés, avec une implication forte des collectivités territoriales, pour développer l'équipement et la mise en réseau des établissements. La démarche de structuration des services numériques mis à la disposition des utilisateurs, engagée notamment à travers des projets tels que les espaces numériques de travail, conduisent les acteurs locaux (services académiques, DRAAF et collectivités territoriales) à inscrire leur collaboration dans une démarche de partenariat global.

Les nouveaux programmes ont, pour la plupart, intégré l'usage des technologies de l'information et de la communication et la culture numérique dans les objectifs et les méthodes d'enseignement et d'apprentissage, tant dans l'enseignement primaire que dans les disciplines de l'enseignement secondaire. Au-delà de son intégration dans les disciplines, la maîtrise de l'usage des outils et des services numériques est devenue une compétence de base du citoyen, tant dans sa vie privée que professionnelle, et cette dimension est prise en compte par le système éducatif.

Dans ce contexte, le Plan numérique lancé par le président de la république en mai 2015 doit permettre aux élèves et aux enseignants de profiter de l'ensemble des opportunités offertes par le numérique.

La volonté de développer le numérique à l'École repose notamment sur le déploiement d'équipements numériques individuels mobiles.

L'arrivée de ces équipements dans les écoles et les établissements, conjointement avec les avancées technologiques comme le cloud ou l'amélioration de la couverture numérique du territoire, va transformer profondément les architectures physiques et logicielles existantes, pour les adapter aux besoins de la pédagogie comme aux contraintes techniques et organisationnelles de mise en œuvre.

Avec un utilisateur connecté en tout lieu de l'école ou de l'établissement, utilisant des ressources multiples et multimédias, les exigences de débit et de disponibilité des services iront croissantes.

Parallèlement, il sera toujours nécessaire d'apporter des garanties concernant le traitement des données personnelles ou la protection des mineurs, pour l'ensemble de la communauté éducative.

La transformation numérique de l'École est en cours. Si le chemin à parcourir pour répondre aux besoins des utilisateurs diffère selon les situations locales, les objectifs sont aujourd'hui clairement définis.

Le référentiel CARINE prend sa place dans le dispositif d'accompagnement du plan numérique pour l'École. Cet outil de référence et de dialogue entre les acteurs académiques et les collectivités territoriales fixe les orientations pour les infrastructures chargées d'accueillir les utilisateurs des services numériques et leurs équipements.

Outre l'existant qui est décrit et traité dans ce référentiel au travers d'une quinzaine de services, le numérique ouvre plus globalement pour le système éducatif des perspectives d'avenir qui permettront d'apprendre autrement.

Mathieu Jeandron

Directeur du numérique pour l'Éducation

1. Objet et positionnement du document

1.1 Préambule

Le présent document a pour objet de fournir le **CA**dre de **R**éférence des services d'**I**nfrastructures **N**umériques d'**É**tablissements scolaires et d'écoles (CARINE). Il annule et remplace la précédente version du cadre de référence des S2i2e de 2008 (CRS2i2e).

Le CARINE constitue le cadre de référence commun aux acteurs décisionnaires des écoles, établissements scolaires, aux inspecteurs d'académie, aux recteurs, aux responsables des collectivités territoriales, ainsi qu'aux éditeurs de solutions et prestataires de services, pour concevoir, choisir, mettre en place et maintenir les infrastructures numériques d'EPLE et d'école.

Il précise les éléments jugés comme suffisamment importants et structurants pour être portés à l'attention de ces différents acteurs.

Le CARINE doit permettre :

- de faciliter le dialogue entre acteurs pour la mise en œuvre des services ;
- de formaliser les exigences en termes de qualité de service ;
- de définir les principes et de préciser les règles qui permettront de favoriser l'interopérabilité des solutions et de faciliter la mutualisation des ressources ;
- de répondre aux nouveaux besoins.

Ce référentiel n'a pas pour vocation de décrire les architectures techniques de mise en œuvre. Il ne préjuge pas notamment de la localisation des services et ne fournit pas de comparaison entre les différentes solutions techniques existantes.

Ces questions sont traitées au niveau territorial par les acteurs locaux de l'éducation et des collectivités, en fonction, entre autre, de la situation existante, des évolutions des usages et des technologies, et de leurs projets de développement du numérique éducatif.

1.2 Concepts et principes fondamentaux

Les services d'infrastructures numériques de l'EPLE ou de l'école ont pour objectif principal la fourniture d'un ensemble de services indispensables à l'accès des services de plus haut niveau[1] dans des conditions de sécurité satisfaisantes.

Ils permettent principalement, la fourniture et la gestion du parc de terminaux (fixes ou mobiles), l'accès authentifié aux postes de travail, puis au réseau de l'établissement ou de l'école et enfin à internet, la mise en œuvre de dispositifs de filtrage destinés à assurer la protection des mineurs dans leurs usages des services numériques (dans le cadre scolaire), ainsi que la supervision, l'exploitation et le maintien en condition opérationnelle de l'ensemble, dans le respect des règles de sécurité applicables et des obligations réglementaires.

Ainsi, les services d'infrastructures numériques doivent permettre la communication interne et l'ouverture du système d'information des collèges, des lycées et des écoles vers l'extérieur dans des conditions de sécurité optimales.

Il importe de prendre en compte, qu'à l'instar de l'expression « système d'information **de** l'EPLE ou **de** l'école », la formulation « services d'infrastructures numériques **de** l'EPLE ou **de** l'école » fait référence à leur finalité et à leurs utilisateurs (la communauté éducative associée) et non pas à une quelconque notion de localisation géographique des matériels et logiciels sous-jacents.

Par conséquent, le CARINE demeure la référence pour les services concernés, qu'ils soient situés dans ou hors l'établissement. Ce point est important à prendre en compte dans un contexte où l'on recherche de plus en plus l'allègement des infrastructures locales.

[1] tels que les outils de gestion du SI des collèges et des lycées, les ENT ou d'autres services spécifiques à un type d'enseignement, à un environnement local particulier.

Les services hors cadre institutionnels, c'est-à-dire choisis, installés et utilisés par les personnels ou les élèves en établissement ou en école ne sont pas abordés dans le CARINE. Le choix d'installer et d'utiliser des services hors périmètre du CARINE :

- par les élèves, relève du domaine du choix individuel, et DOIT se faire sous l'autorité des parents pour les mineurs ; il n'y a pas de prescription institutionnelle possible dans ce cadre ;
- par les personnels, relève du domaine du choix individuel ; leur responsabilité est alors engagée sur l'usage qui en est fait.

1.3 Positionnement dans le corpus référentiel

Le cadre de référence CARINE n'est pas un document isolé, il s'articule avec d'autres référentiels qui précisent le contexte dans leur domaine respectif, notamment le cadre de référence CARMO et le SDET qui s'inscrivent dans le plan d'ensemble destiné à accompagner le développement du numérique éducatif.

Plusieurs documents précisent actuellement domaine par domaine les besoins des acteurs du système éducatif. Sans chercher à être exhaustif on peut citer :

- le présent référentiel CARINE ;
- le SDET, schéma directeur des espaces numériques de travail, qui définit un bouquet de services à destination des utilisateurs des 1er et 2d degrés ;
- les référentiels d'équipement qui permettent d'évaluer et de projeter les besoins matériels d'une école ou d'un établissement du 2^{d} degré ;
- le Cadre de référence pour l'Accès aux Ressources pédagogiques via un équipement Mobile (CARMO) pour l'utilisation de terminaux mobiles de type tablettes notamment, et affectés aux élèves de façon individuelle ;
- des référentiels thématiques (référentiel Wi-Fi, par exemple) ;
- les référentiels interministériels (RGI[2], RGS[3], PSSIE[4]…).

Le schéma ci-après représente une vision urbanisée du CARINE et des principaux référentiels connexes. Il apporte plusieurs éclairages, parmi lesquels :

- les interactions entre le CARINE et le SDET :

  5 services rendus aux utilisateurs (stockage, messagerie électronique, communication temps réel, publication et recherche documentaire) sont décrits dans CARINE. Ce référentiel apporte, pour ces 5 services, des éléments considérés comme indispensables a minima. Lors de la mise en place de l'ENT, l'articulation des services d'infrastructures numériques et des services délivrés par l'ENT doit être étudiée.

- les interactions entre le CARINE et le CARMO :

  Le CARMO a pour objectif de fournir le Cadre de référence national pour l'Accès aux Ressources pédagogiques via un équipement Mobile dans le cadre de projets visant à équiper les membres de la communauté éducative de l'établissement (en particulier les élèves et leurs enseignants). Le CARINE permet d'assurer la cohérence globale avec les infrastructures d'EPLE et d'écoles destinées à accueillir ces utilisateurs et leur équipement.

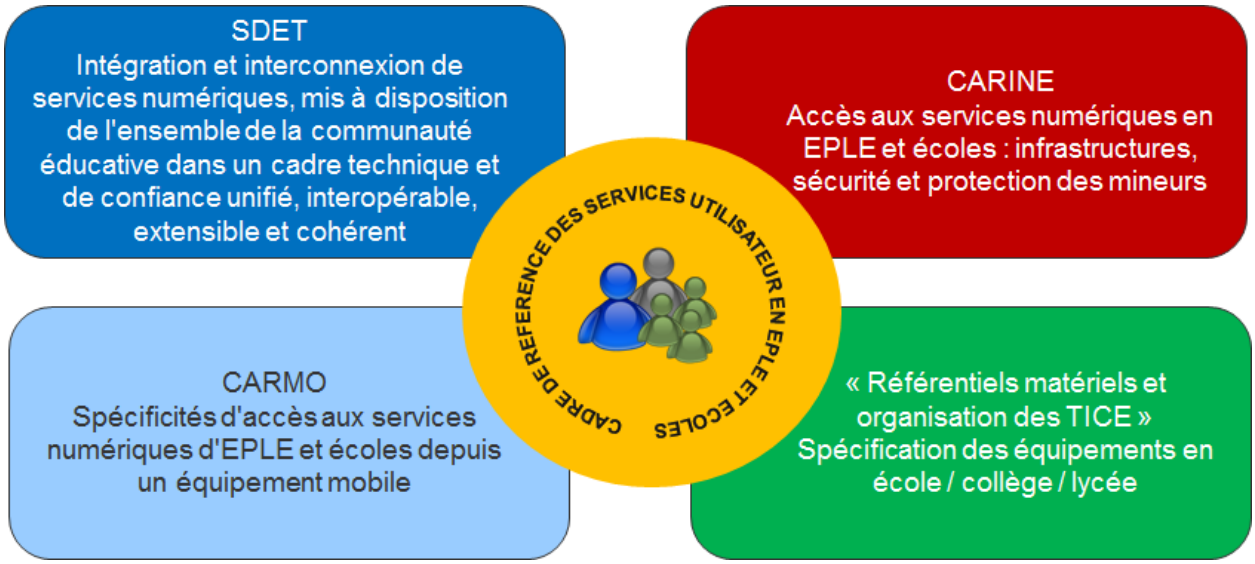
- le positionnement central des services rendus aux utilisateurs :

  Les services rendus aux utilisateurs, leur qualité et leur adaptation aux besoins métier constituent la finalité des projets d'infrastructures, d'équipement et de développement d'environnements de travail modernes, interopérables et extensibles. Ils sont donc présents à différents niveaux des référentiels existants. Dans le cadre de sa réflexion sur l'urbanisation des référentiels, le ministère projette de mettre en place un *Cadre de référence des services utilisateur en EPLE et écoles* qui sera consacré à la description fonctionnelle des « services métier » ; ce nouveau découpage augmentera la lisibilité de l'ensemble et diminuera les couplages « parasites » entre référentiels, simplifiant ainsi leur mise à jour.

[2] Référentiel Général d'Interopérabilité

[3] Référentiel général de sécurité

[4] Politique de sécurité des systèmes d'information de l'État



1.4 Les compléments du CARINE

Le « cœur de référentiel » CARINE, c'est-à-dire le présent document, n'a pas pour objet de fournir des références techniques ou des modèles d'implémentation. Afin d'accompagner les porteurs de projets en académies, le ministère complètera ce cœur selon les besoins avec :

- des référentiels thématiques ;
- des retours d'expériences.

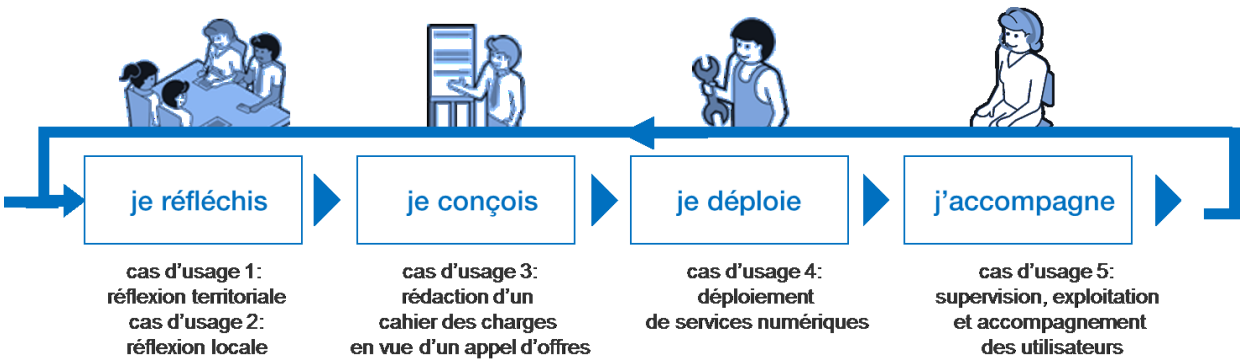
Le *Référentiel sur l'usage du Wi-Fi en établissement et école* constitue un exemple de référentiel thématique CARINE. D'autres devraient le rejoindre prochainement. Parmi les sujets candidats on peut noter :

- mobilité et BYOD (en relation avec le CARMO) ;
- messagerie scolaire ;
- protection des mineurs et filtrage ;
- les identités et leur gestion...

Par ailleurs, le passage au web des référentiels (voir chapitre suivant) permettra de mettre en place un partage des retours d'expérience en académies en lien avec les thèmes ou les services d'infrastructures traités dans le référentiel.

1.5 Utilisation du référentiel

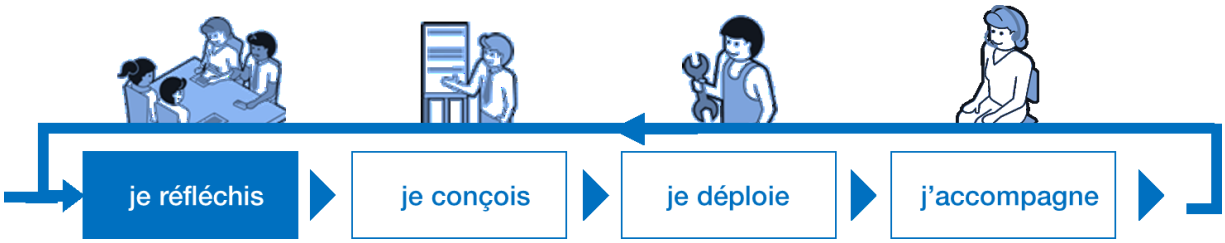
Le CARINE peut être utilisé à chaque grande étape du cycle de vie d'un projet numérique en environnement scolaire, du cadrage de la stratégie à la gestion opérationnelle. Pour illustrer cette dimension temporelle des projets, 5 cas d'usage sont donnés ci-après à titre d'illustration.



Les acteurs concernés par les services d'infrastructures numériques dans les établissements scolaires et les écoles ne sont pas tous mobilisés sur chacun de ces cas d'usage. Toutefois, dans un objectif d'efficience et de qualité du service rendu, il est indispensable d'avoir une vision globale des sujets abordés :

- un acteur mobilisé sur les phases amont de stratégie et de réflexion doit anticiper la faisabilité et l'exploitabilité des scénarios envisagés ;
- un acteur mobilisé sur les phases aval de déploiement et d'accompagnement doit comprendre les objectifs et les enjeux associés au service mis en œuvre.

1.5.1 Cas d'usage n°1 : réflexion académique et territoriale

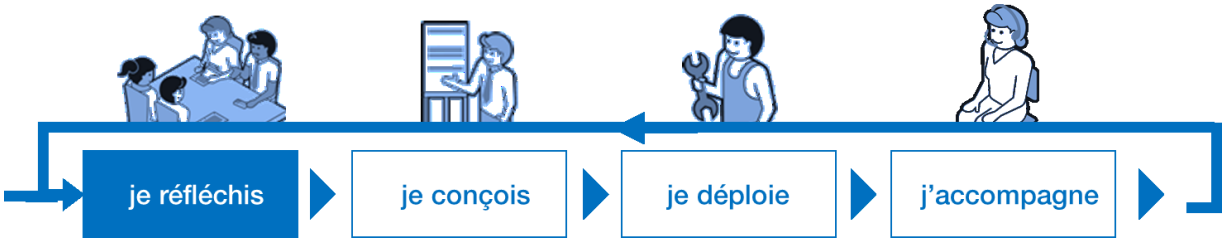


En prévision d'une réunion de coordination sur la politique numérique éducative entre les services académiques (ou la DRAAF pour l'enseignement agricole) et les collectivités, vous devez identifier les besoins, moyens et préconisations liés aux infrastructures numériques.

Dans ce contexte, le CARINE peut vous aider à construire vos argumentaires sur des sujets tels que :

- raccordement d'un établissement/d'une école au haut débit ;
- déploiement d'une infrastructure Wi-Fi dans un établissement/une école ;
- qualification des besoins de sécurité ;
- définition des modalités d'hébergement des services ;
- exploitation, supervision, maintien en condition opérationnelle ;
- équipement en terminaux fixes et mobiles ;
- prise en compte des équipements personnels (BYOD).

1.5.2 Cas d'usage n°2 : réflexion locale



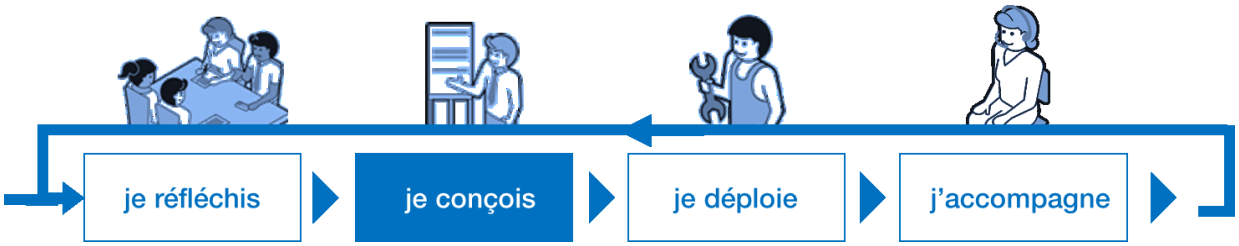
Dans le cadre de la stratégie numérique mise en place par la collectivité et les services académiques (ou la DRAAF pour l'enseignement agricole), vous êtes amené :

- en tant que chef d'établissement, directeur d'école ou IEN de circonscription, à formaliser des besoins métiers (pédagogie, gestion) en prévision de l'intégration de services numériques de l'établissement ou de l'école ;
- en tant que porteur des sujets numériques en collectivité ou dans les services académiques ou la DRAAF, à arbitrer les projets à mettre en œuvre en fonction de la stratégie définie et des capacités techniques requises.

Dans ce contexte, le CARINE peut vous aider à construire vos argumentaires sur des sujets tels que:

- expression des besoins métier ;
- raccordement de l'établissement ou de l'école au haut-débit ;
- déploiement d'une infrastructure Wi-Fi ;
- équipement en terminaux fixes ou mobiles ;
- prise en compte des équipements personnels (BYOD).

1.5.3 Cas d'usage n°3 : rédaction d'un appel d'offres



Dans le cadre du développement des services numériques dans un établissement ou une école, vous êtes amené à rédiger un cahier des charges pour éventuellement publier des appels d'offres et/ou à faire des choix pour l'acquisition et la mise en œuvre de matériels et services tels que :

- infrastructures (sécurité, serveurs, réseau, stockage, réseau sans-fil…) ;
- terminaux fixes ou mobiles (ordinateurs fixe, ordinateurs portable, ordiphone…), mutualisés ou individuels ;
- services numériques et outils logiciels (suite bureautique, logiciels vidéo, audio…).

Dans ce contexte, le CARINE peut vous aider à construire votre cahier des charges pour la consultation.

Dans le cadre d'un projet d'équipement mobile le lecteur se reportera également au référentiel CARMO afin d'y trouver une information spécifique sur les terminaux mobiles et leur gestion, le déploiement et la gestion des applications mobiles, etc.

1.5.4 Cas d'usage n°4 : déploiement des services numériques

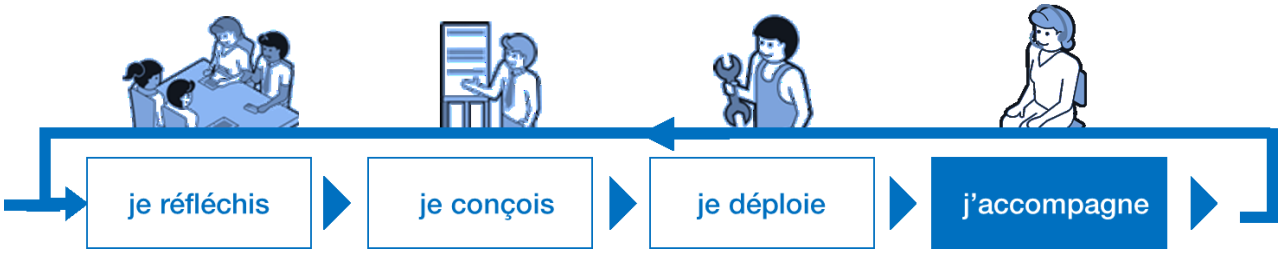
Faisant suite à l'attribution des marchés, la mise en œuvre des services va être initiée en lien avec l'ensemble des parties prenantes :

- services académiques (ou la DRAAF pour l'enseignement agricole) ;
- établissements concernés ;
- collectivités de rattachement ;
- prestataires.

Dans ce contexte, afin de préparer l'intégration et le déploiement auprès des utilisateurs de nouveaux matériels et/ou services vous devez traiter tout ou partie des sujets suivants :

- l'intégration d'équipements individuels mobiles dans l'écosystème existant ;
- l'intégration de services numériques (hors ENT) dans l'écosystème existant (métier + infrastructures) ;
- l'intégration d'un ENT dans l'écosystème existant (métier + infrastructures) ;
- la phase de test et de recette de la solution, qui valide le déploiement ;
- l'exploitation et la maintenance des services et infrastructures numériques.

1.5.5 Cas d'usage n°5 : supervision, exploitation et accompagnement des utilisateurs



Suite à la mise en œuvre d'un service numérique en établissement ou en école, le service passe en phase opérationnelle.

Dans ce contexte, vous pourriez avoir à définir et organiser les tâches suivantes :

- l'accompagnement et le support aux utilisateurs ;
- la sensibilisation à la sécurité ;
- la définition des règles d'exploitation et de supervision, ainsi que la répartition des responsabilités attachées ;
- l'exploitation et la maintenance du service numérique.

2. Contenu, présentation et principales nouveautés

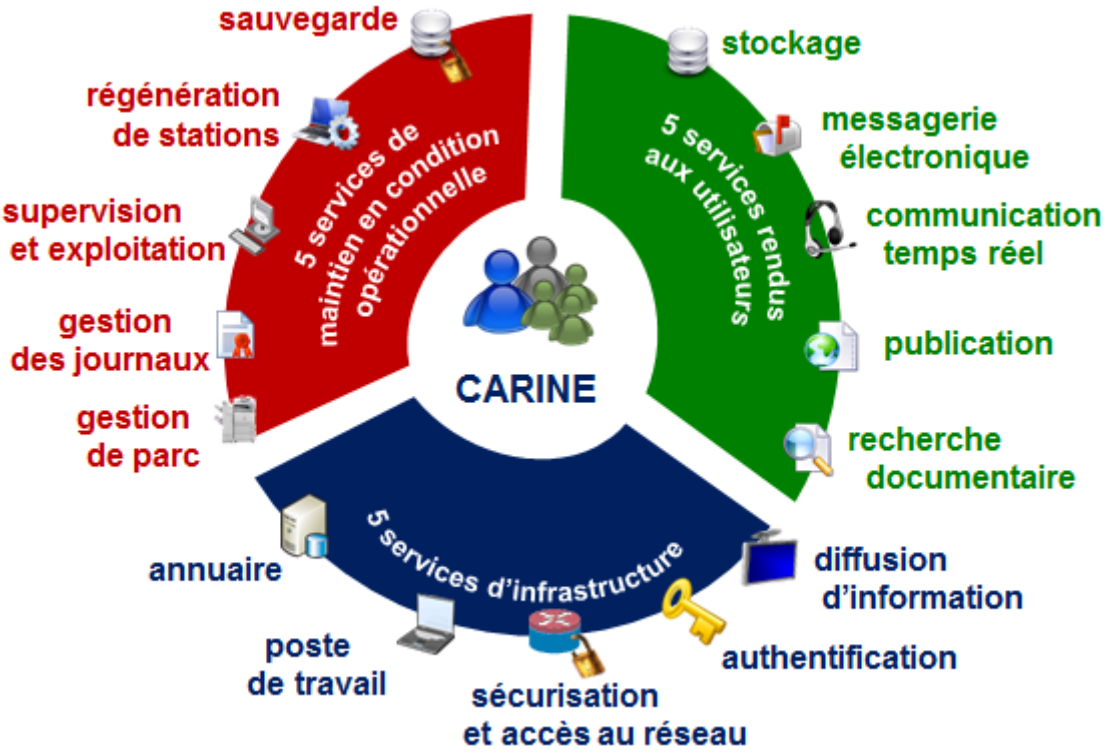
2.1 Contenu et principales nouveautés

Les 15 services décrits dans le CARINE se répartissent en 3 catégories. Deux d'entre elles sont relatives aux infrastructures matérielles et logicielles, proprement dites ; il s'agit des services d'infrastructures et des services de maintien en condition opérationnelle. La troisième catégorie concerne 5 services utilisateur considérés comme indispensables.

La présence des services utilisateur de base trouve sa raison dans l'histoire du référentiel S2i2e, dans le fait qu'actuellement il n'existe pas de référentiel dédié aux services utilisateur et que, par ailleurs, les ENT ne sont pas encore déployés partout, notamment dans le premier degré.

En conséquence, le CARINE apporte des éléments considérés comme indispensables a minima en ce qui concerne les services aux utilisateurs. Lors de la mise en place de l'ENT, l'articulation des services d'infrastructures numériques et des services délivrés par l'ENT doit être étudiée.

Les 15 services du CARINE :



Les principales nouveautés portent tant sur les contenus que sur la forme.

On y trouve ainsi 3 nouveaux services :

- le *service poste de travail* est désormais pris en compte au sein d'un service spécifique qui aborde la dimension fourniture et cycle de vie ;
- un *service de diffusion d'information* a été ajouté pour prendre en compte le service lié à l'installation d'équipements d'affichage numérique dans les espaces publics ou communs de l'établissement ou de l'école ;
- le *service de gestion de parc* vient compléter les services de maintien en condition opérationnelle.

Les aspects juridiques sont davantage mis en avant que dans le référentiel précédent et ont vocation à être étoffés et précisés dans les versions futures.

La dimension organisationnelle est également étoffée, notamment en lien avec les questions de sécurité et les aspects juridiques.

Enfin, l'amorce d'un recentrage du référentiel sur les infrastructures numériques de l'EPLE ou de l'école, dans une vision urbanisée des référentiels, se traduit par le changement de nom et se verra poursuivie dans les versions ultérieures, en liaison avec le processus d'urbanisation.

2.2 Organisation et conventions d'écriture

Outre les chapitres introductifs, le CARINE comprend un chapitre traitant de façon détaillée les 15 services listés plus haut. Il est suivi d'un historique permettant de comprendre comment on est passé de la vision de la note de cadrage de 2002 au référentiel actuel. Le glossaire, en fin d'ouvrage, reprend les définitions des sigles, mots et expressions correspondant aux acceptions de ces termes dans le présent référentiel.

Chaque description de service est subdivisée en 7 parties permettant au lecteur de repérer plus rapidement les différentes thématiques et d'organiser ainsi sa lecture en fonction de la nature des d'informations recherchées.

Ces 7 parties sont les suivantes :

- introduction présentant rapidement le service ;
- impacts du service sur les infrastructures ;
- impacts sur l'organisation de l'EPLE ou de l'école ;
- impacts sur la sécurité des systèmes d'information ;
- aspects juridiques ;
- un tableau soulignant les relations d'interaction entre services ;
- un tableau récapitulatif des recommandations effectuées dans le texte.

Les recommandations sont fournies en suivant la terminologie définie dans le RFC 2119 de l'IETF[5]. Ce formalisme est signalé par les mots suivants écrits en lettres capitales dans le texte :

- **DOIT** : ce mot, ou l'adjectif « **EXIGÉ** », signifie que la définition est une exigence absolue de la spécification.
- **NE DOIT PAS** : cette expression signifie que la définition est une prohibition absolue de la spécification.
- **DEVRAIT** : ce mot, ou l'adjectif « **RECOMMANDÉ** », signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer cet item particulier, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente.
- **NE DEVRAIT PAS** : ce mot, ou l'adjectif « **NON RECOMMANDÉ** », signifie que la définition est prohibée. Il peut toutefois exister des raisons valables, dans des circonstances particulières, quand le comportement ainsi défini est acceptable ou même utile, de ne pas suivre cette recommandation. Mais les conséquences doivent être comprises et le cas soigneusement pesé.
- **PEUT** : Ce mot, ou l'adjectif "**FACULTATIF**", signifie qu'un élément est facultatif. Cela signifie que la présence de l'élément en question améliore le service, mais que son absence n'empêche pas le service d'être rendu.

Notez que la force de ces mots est également fonction du niveau d'exigence représenté par le document lui-même, ainsi que par les éventuelles normes qui fondent certaines de ces dernières. C'est pourquoi le CARINE voit sa composante juridique étoffée par rapport au CRS2i2e qui l'a précédé.

2.3 Format et présentation

Le référentiel CARINE vous est présenté ici sous forme d'un fascicule paginé et imprimable.

Par ailleurs, le ministère projette de porter progressivement ses référentiels sous forme de dossiers web afin de faciliter les mises à jour, ainsi que la navigation entre les différents éléments de l'ensemble, y compris les référentiels connexes et les compléments évoqués dans la section « *Les compléments du CARINE* » au chapitre précédent.

[5] https://www.ietf.org/rfc/rfc2119.txt

3. Références des services

3.1 Structure des fiches services

Chaque service est décrit en 2 parties :

- Une fiche synthétique qui donne un aperçu global du service rendu avec :
    - Le besoin ;
    - Les impacts sur les infrastructures ;
    - Les impacts sur l'organisation ;
    - Les impacts sur la sécurité ;
    - Les aspects juridiques importants dont la protection des mineurs ;
    - Les interactions avec les autres services d'infrastructure.
- Un tableau de fonctionnalités qui détaille une à une les fonctionnalités exigées, recommandées et facultatives.

Légende pour la lecture des tableaux de description des services :

Les services du CARINE doivent offrir un certain nombre de fonctions et/ou répondre à des exigences particulières qui sont exprimées dans ces tableaux.

Un service est caractérisé par un code d'identification et un libellé.

Il regroupe un ensemble de fonctions, déclinées en fonctionnalités et répondant à certaines règles. Ces fonctions sont détaillées sous forme de tableaux.

Trois niveaux de préconisation s'appliquent aux fonctionnalités :

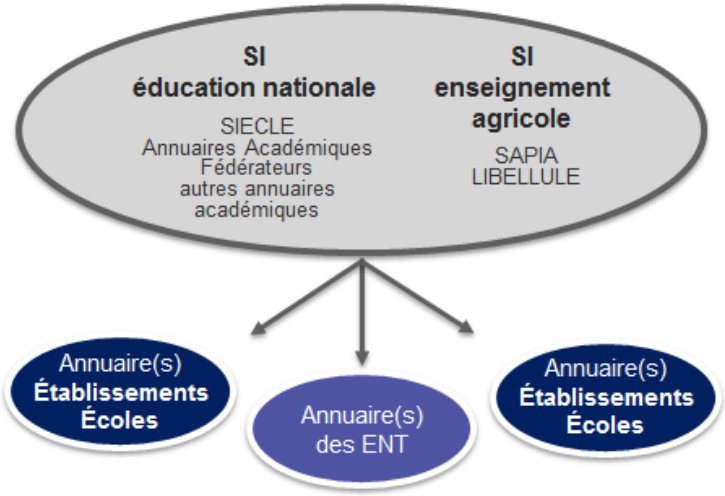
- Le niveau « E-exigé », appliqué à une fonctionnalité et/ou règle de gestion, signifie que le service correspondant DOIT offrir ladite fonctionnalité.
- Le niveau « R-recommandé », appliqué à une fonctionnalité et/ou règle de gestion, signifie que le service correspondant DEVRAIT offrir ladite fonctionnalité. La décision de ne pas fournir la fonctionnalité ou de ne pas respecter la règle de gestion doit être pesée dans toutes ses conséquences (pédagogique, administrative, juridique et/ou organisationnelle) et dument justifiée auprès des acteurs concernés.
- Le niveau « F-facultatif » appliqué à une fonctionnalité et/ou règle de gestion, signifie qu'il est souhaitable d'appliquer cette recommandation mais qu'il peut exister des éléments de contexte rendant son application difficilement réalisable ou disproportionnée par rapport aux enjeux et aux objectifs prioritaires assignés au projet.

3.2 Services d'infrastructure

3.2.1 Service d'annuaire

Service d'annuaire

Du fait de la responsabilité juridique liée à la fourniture d'accès au réseau et à internet ainsi qu'au caractère personnel de certains espaces de travail, tout utilisateur DOIT être identifié et authentifié (voir **service d'authentification**) de façon unique avant d'accéder aux ressources. Cela nécessite la mise en œuvre d'annuaires d'identités (annuaires académiques, annuaires ENT) et d'annuaires d'infrastructure en établissement/école.



Impacts sur les infrastructures

Le service d'annuaire d'infrastructure de l'établissement ou de l'école, fournit un référentiel qui permet l'identification des utilisateurs dans le but de contrôler l'accès aux terminaux informatiques et aux réseaux, de gérer et personnaliser ces terminaux et leurs applications et de permettre une gestion adaptée de l'accès aux services locaux (serveurs de fichiers, imprimantes…).

Processus d'échange : L'annuaire ENT est alimenté automatiquement et régulièrement à partir de l'annuaire académique fédérateur (AAF), lui-même alimenté à partir des bases de gestion (SIECLE, STSWEB, BE1D, RAMSESE, EPP, AGORA, AGAPE, ou encore SAPIA, LIBELLULE, FREGATA pour l'enseignement agricole), en ce qui concerne les élèves, les parents et tous les personnels affectés à l'établissement/école.

Processus d'interrogation : Le service d'annuaire DOIT offrir des mécanismes standard d'interrogation et de recherche (requêtes) sur les annuaires d'infrastructure d'établissements/d'écoles.

Processus d'import/export : Le service d'annuaire DOIT offrir des mécanismes standard d'import/export (réplication/synchronisation) pour permettre l'alimentation des annuaires d'infrastructure d'établissements/d'écoles à partir d'un annuaire académique (solution à privilégier) ou de celui de l'ENT (voir **ensemble annuaire de l'annexe opérationnelle du SDET** – version à paraître à la rentrée 2016). Cette synchronisation entre annuaires DOIT être sécurisée (réalisée dans une zone sécurisée et/ou via des échanges sécurisés).

Impacts sur l'organisation

Les processus d'échange entre les annuaires académiques, les bases de gestion, l'annuaire ENT et les annuaires d'infrastructures d'établissement/d'école sont définis par le ministère.

Les éventuels besoins d'interaction avec les annuaires des collectivités territoriales doivent être étudiés en collaboration avec ces dernières, dans l'objectif de permettre l'interopérabilité des systèmes d'information, tout en respectant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La personne responsable des traitements de données à caractère personnel contenues dans les annuaires d'infrastructure peut déléguer tout ou partie de la responsabilité opérationnelle à une ou des personnes identifiées de manière claire (information des personnes concernées par les traitements).

Impacts sur la sécurité des SI

En établissement/école, hormis l'annuaire ENT et les bases de gestion SIECLE ou BE1D, les référentiels d'identité NE DOIVENT PAS contenir de données détaillées relatives à l'identité ou à la vie privée des utilisateurs (date de naissance, téléphone, adresse, responsables légaux, etc.).

Les flux d'alimentation et de réplication des annuaires ne DOIVENT transiter que sur des réseaux sécurisés ou via des protocoles chiffrés.

Toute modification ou tentative de modification d'un annuaire DOIT être tracée, identifiée et horodatée. (voir **service de gestion des journaux)**

Aspects juridiques

La constitution d'un annuaire sur support informatisé comportant l'identité des personnes, leur fonction, leurs coordonnées professionnelles et le cas échéant leur photographie, constitue un traitement de données à caractère personnel soumis aux dispositions de la loi du 6 janvier 1978 modifiée en 2004.

Les annuaires d'infrastructure PEUVENT être alimentés à partir de référentiels d'identité préexistants, notamment depuis un annuaire académique (solution à privilégier) mais ne DOIVENT reprendre que les données strictement nécessaires à leurs fonctions. Plusieurs sources de données peuvent être envisagées[6], en fonction du contexte académique, et selon les besoins réels des annuaires d'infrastructures :

- l'annuaire ENT, sous réserve qu'il soit fourni dans le cadre d'un partenariat État – collectivité territoriale et que l'engagement de conformité au RU-003 ait été réalisé par le responsable de traitement ;
- l'Annuaire Académique Fédérateur (AAF), sous réserve qu'il fasse l'objet d'une extraction spécifique ;
- SIECLE, BE1D[7].

Les responsables des projets d'infrastructures sont invités à vérifier le cadre juridique avant d'utiliser l'une de ces sources de données, les modifications juridiques nécessaires étant en cours.

L'alimentation à partir d'autres référentiels que ceux cités dans la présente section DOIT faire l'objet de formalités complémentaires auprès de la CNIL, dans la mesure où ce circuit n'est pas couvert par le cadre national mis en place.

À terme, des solutions permettant l'automatisation de l'alimentation des annuaires d'infrastructure, à partir de référentiels existants et uniquement en données strictement nécessaires, seront proposées par l'éducation nationale (projet en cours).

Les annuaires d'infrastructure contiennent des données à caractère personnel. Le chef d'établissement / le DASEN[8] est responsable de ces données sur le périmètre de son établissement / de son département.

il est conseillé de consulter régulièrement la rubrique « éducation » sur le site de la CNIL et de contrôler le niveau de conformité de l'établissement ou de l'école avec les fiches pratiques diffusées sur www.cnil.fr.

http://eduscol.education.fr/internet-responsable/textes-legislatifs-et-reglementaires.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/image-et-video.html

Interaction avec d'autres services

☐ annuaire	☐ sauvegarde	☒ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☒ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

6 Dans l'attente d'une documentation détaillée, des précisions seront fournies aux académies par circulaire pour accompagner la rentrée 2016 et la mise en œuvre au cours de l'année scolaire 2016-2017.

7 Alimentation depuis SIECLE, BE1D : cette option nécessite une saisie, dans les annuaires, des données des enseignants

8 Directeur académique des services de l'Éducation nationale

INF-ANN Service d'annuaire

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
INF-ANN-1	Identification	Tout utilisateur DOIT être identifié (via le service d'annuaire) et authentifié (via le service d'authentification) avant l'accès aux ressources.	E	E
INF-ANN-2	Requêtes	Le service d'annuaire DOIT offrir des mécanismes standard d'interrogation et de recherche (requêtes) sur les annuaires d'infrastructure d'établissements/d'écoles.	E	E
INF-ANN-3	Alimentation	Le service d'annuaire DOIT offrir des mécanismes standard d'import/export (réplication / synchronisation) pour permettre l'alimentation des annuaires d'infrastructure d'établissements/d'écoles à partir d'un annuaire académique (solution à privilégier) ou de celui de l'ENT.	E	E
INF-ANN-4	Traçabilité	Toute modification ou tentative de modification d'un annuaire DOIT être tracée, identifiée et horodatée.	E	E
INF-ANN-5	Import/Export	Les flux d'alimentation et de réplication des annuaires ne DOIVENT transiter que sur des réseaux sécurisés ou via des protocoles chiffrés.	E	E
INF-ANN-6	Import/Export	Les annuaires d'infrastructure PEUVENT être alimentés à partir de référentiels de données préexistants, notamment depuis un annuaire académique (solution à privilégier) mais ne DOIVENT reprendre que les données strictement nécessaires à leurs fonctions.	E	E
INF-ANN-7	Contenu	L'alimentation à partir d'autres référentiels que ceux cités dans la présente section DOIT faire l'objet de formalités complémentaires auprès de la CNIL, dans la mesure où ce circuit n'est pas couvert par le cadre national mis en place.	E	E
INF-ANN-8	Contenu	En établissement/école, hormis l'annuaire ENT et les bases de gestion SIECLE ou BE1D, les référentiels d'identité NE DOIVENT PAS contenir de données détaillées relatives à l'identité ou à la vie privée des utilisateurs (date de naissance, téléphone, adresse, responsables légaux, etc.).	E	E

3.2.2 Service poste de travail

Service poste de travail

L'utilisateur accède aux services numériques à l'aide d'un poste de travail, qui peut être fixe ou mobile.

*Pour les terminaux mobiles, se référer au **dossier CARMO**.*

Impacts sur les infrastructures

Le service poste de travail fournit le ou les terminaux permettant l'accès aux services numériques. Cela inclut les postes fixes et mobiles.

Poste partagé

Dans le cas où le poste est partagé entre plusieurs utilisateurs, le service de régénération et de configuration de stations DEVRAIT être activé. Il est nécessaire de définir clairement les procédures de régénération ou de reconfiguration du poste, la qualité de service attendue (notamment au regard des délais de traitement), et le traitement réservé aux données locales. (voir **service de régénération et de configuration de stations)**.

Un poste fixe partagé DEVRAIT faire l'objet d'une procédure d'arrêt automatique en fin de journée.

Type de poste : Les postes de travail PEUVENT être en configuration client lourd (poste classique avec son stockage et ses applications), client léger (données et applications distantes), voire ultra léger/zéro client (mode terminal passif).

Si elles sont utilisées, les techniques de déport des applications (virtualisation par exemple) DOIVENT tenir compte des contraintes de débit réseau et des impacts sur l'infogérance (gestion des accès, des serveurs de distribution, des impressions…).

Configuration du poste : Dans un objectif de qualité de service, de sécurité et de simplification de l'infogérance, les configurations des postes de travail DEVRAIENT être « masterisées ». Lorsque les débits réseau le permettent, les techniques utilisées devraient privilégier les outils de télédistribution à distance. (voir **service de régénération et de configuration de station**).

Les personnes en situation de handicap DOIVENT être équipées de postes adaptés.
http://eduscol.education.fr/cid56843/ressources-numeriques-adaptees-soutenues-et-realisees.html

Impacts sur l'organisation

La typologie des postes de travail doit être définie par le ministère en collaboration avec les collectivités territoriales. Cette typologie doit correspondre au profil des utilisateurs (personnels, élèves), à leur usage pédagogique ou administratif et à leur situation d'usage (fixe, mobilité). Pour les personnels d'encadrement et de direction, elle devrait déboucher sur une liste d'équipements parmi lesquels l'utilisateur pourra choisir celui qui correspond le mieux à ses usages.

Un poste de travail peut contenir des données personnelles, voire privées, d'un utilisateur. L'utilisateur DOIT identifier ces données en les marquants par les mots "PERSONNEL" ou "PRIVÉ" (voir **service de stockage**). Alternativement ou de façon complémentaire ce répertoire peut être créé avec une autre règle de nommage par l'administrateur du système. Son emplacement et la règle de nommage associée devront être précisés de façon explicite dans les CGU du service.

Les utilisateurs doivent être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau. (Cf. recommandations et fiches pratiques CNIL : https://www.cnil.fr/fr/10-conseils-pour-la-securite-de-votre-systeme-dinformation).

Les postes de travail ayant une durée de vie limitée (6 ans en moyenne), leur remplacement et leur mise au rebut devraient être anticipés (voir **service de gestion de parc**).

Les postes des personnels de direction et des gestionnaires DEVRAIENT pouvoir être remplacés en un jour ouvré (ex : provision de postes prêts à l'emploi).

Cela DEVRAIT être également le cas pour les élèves à besoins éducatifs particuliers pour qui l'ordinateur est souvent un moyen pour appréhender le monde et/ou communiquer.

« BYOD »

Les postes de travail privés des personnels PEUVENT être utilisés dans l'établissement/l'école (BYOD – Bring Your Own Device- ou AVEC en français – Apportez Votre Équipement personnel de Communication). Dans ce cas, la politique de sécurité de l'établissement et le règlement intérieur DEVRAIENT décrire précisément les modalités d'accès ainsi que les limites de responsabilités (ex : assurance, responsabilité juridique vis-à-vis des usages, etc.). Un paragraphe spécifique DEVRAIT également être ajouté à la charte de l'établissement / de l'école (ex : propriété, vie privée, responsabilité juridique vis-à-vis des usages, etc.).

Les élèves à besoins éducatifs particuliers doivent pouvoir utiliser un poste de travail :

- soit notifié par les MDPH et prêté par les académies ;
- soit acheté par les parents.

Ces postes de travail sont souvent équipés de périphériques particuliers : plages braille, claviers spéciaux, dispositifs de pointage adaptés (capteurs), scanners portables, webcams…

Poste partagé

Le partage d'un poste de travail PEUT avoir des impacts sur l'organisation. Les règles d'usage, en particulier les droits d'accès au poste, sont définies par les équipes pédagogiques. Les utilisateurs DOIVENT être sensibilisés au processus de partage des postes de travail et formés au mécanisme de régénération de configuration et à ses impacts (voir **service de régénération et de configuration de stations**). Cette information DOIT figurer dans la charte de l'établissement/école ou dans les CGU du service.

Impacts sur la sécurité des SI

Sécurité du poste : Les postes de travail DOIVENT être sécurisés, c'est à dire a minima imposer une authentification pour l'accès au poste et contenir un antivirus. Ils DEVRAIENT contenir un mécanisme de filtrage des flux (« pare feu individuel »). (voir **service d'authentification)**

Les postes de travail DEVRAIENT être paramétrés afin qu'ils se verrouillent ou ferment la session en cours automatiquement au-delà d'une période d'inactivité.

Les postes en libre-service DOIVENT être configurés pour ne donner accès qu'à des services non sensibles. Ces postes NE DOIVENT PAS contenir de données personnelles.

Sécurité des données : Si des données administratives sont malgré tout stockées sur le poste de travail des personnels non enseignants (personnels de direction, personnels administratifs…) ou du directeur d'école, ces données doivent être protégées ; Elles PEUVENT être chiffrées (chiffrement de masse) (voir **service de stockage**) et DOIVENT être sauvegardées (voir **service de sauvegarde**). Pour les utilisateurs concernés par le mécanisme de chiffrement, il faut les mettre en garde contre les pertes de données qui peuvent résulter d'une perte des moyens d'accès à leur compte.

Droits d'administration : Donner aux utilisateurs les droits administrateurs sur le poste de travail peut avoir des conséquences lourdes sur les processus de maintenance et de maintien en condition opérationnelle. Il faut cependant veiller à ce que les postes utilisés par des personnes en situation de handicap permettent toutes les adaptations nécessaires, notamment la prise en compte de leurs périphériques spécifiques personnels.

Pour permettre l'installation d'outils numériques hors catalogue par les personnels, d'autres solutions PEUVENT être préférées (ex : poste réservé à l'innovation et au test de nouveaux outils, machine virtuelle préinstallée sur le poste…).

D'une façon générale, une politique de sécurité liée à l'administration des postes de travail doit être définie et formalisée.

Mise au rebut : Lors de la mise au rebut, la récupération puis la suppression définitive des données sur le poste doivent être programmées. Cela peut nécessiter de mettre à disposition temporairement des locaux dédiés à la

récupération des anciens postes et à la préparation des nouveaux.

Aspects juridiques

Les élèves à besoins éducatifs particuliers DOIVENT pouvoir disposer d'un poste de travail adapté lors des examens.

http://www.education.gouv.fr/pid285/bulletin_officiel.html?cid_bo=91832

Le traitement des postes obsolètes est régi par le code de l'environnement, publié pour sa partie législative en annexe de l'Ordonnance n° 2000-914 du 18 septembre 2000 (JO du 21 septembre 2000).

http://eduscol.education.fr/internet-responsable/textes-legislatifs-et-reglementaires.html

Interaction avec d'autres services

☒ annuaire	☒ sauvegarde	☒ stockage / synchronisation
☐ poste de travail	☒ régénération de configurations	☐ messagerie électronique
☒ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☐ publication
☐ diffusion d'information	☒ gestion de parc	☐ recherche documentaire

INF-PDT Service poste de travail

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
INF-PDT-1	Approvisionnement	Les postes des personnels de direction et des gestionnaires DEVRAIENT pouvoir être remplacés en un jour ouvré (ex : provision de postes prêts à l'emploi). Cela DEVRAIT être également le cas pour les élèves à besoins éducatifs particuliers.	R	R
INF-PDT-2	Configuration	Les postes de travail PEUVENT être en configuration client lourd (poste classique avec son stockage et ses applications), client léger (données et applications distantes), voire ultra léger/zéro client (mode terminal passif).	F	F
INF-PDT-3	Configuration	Dans un objectif de qualité de service, de sécurité et de simplification de l'infogérance, les configurations des postes de travail DEVRAIENT être « masterisées ».	R	R
INF-PDT-4	Stockage	Un poste de travail peut contenir des données personnelles, voire privées, d'un utilisateur. L'utilisateur DOIT identifier ces données en les marquants par les mots "PERSONNEL" ou "PRIVÉ". Alternativement ou de façon complémentaire ce répertoire peut être créé avec une autre règle de nommage par l'administrateur du système. Son emplacement et la règle de nommage associée devront être précisés de façon explicite dans les CGU du service.	E	E
INF-PDT-5	Droits administrateur	Le poste de travail DEVRAIT être fourni configuré de sorte que l'utilisateur n'ait pas les droits d'administration sur le poste.	R	R
INF-PDT-6	Droits administrateur	Pour permettre l'installation d'outils numériques hors catalogue par les personnels, d'autres solutions que celle de donner les droits administrateur à l'utilisateur PEUVENT être préférées (ex : poste réservé à l'innovation et au test de nouveaux outils, machine virtuelle préinstallée sur le poste…).	F	F
INF-PDT-7	Sécurité du poste	L'accès au poste de travail DOIT être soumis à authentification.	R	E
INF-PDT-8	Sécurité du poste	Un antivirus DOIT être installé sur le poste de travail.	E	E

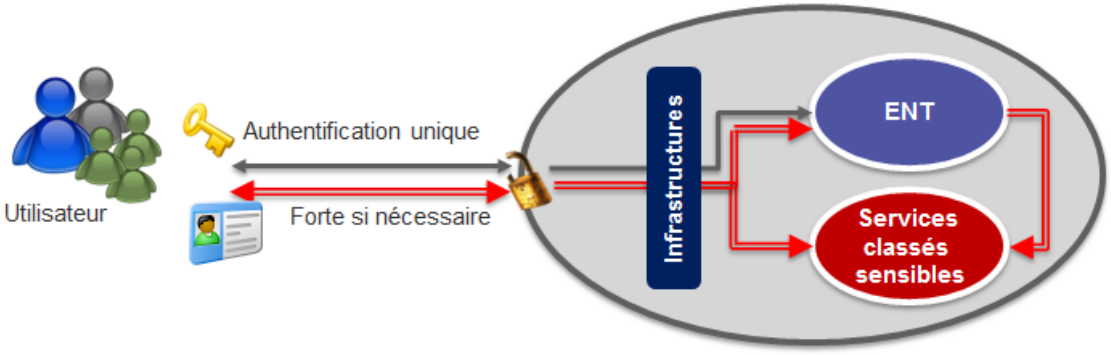
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
INF-PDT-9	Sécurité du poste	Les postes de travail DEVRAIENT contenir un mécanisme de filtrage des flux (« pare feu individuel »).	R	R
INF-PDT-10	Sécurité	Les postes de travail DEVRAIENT être paramétrés afin qu'ils se verrouillent ou ferment la session en cours automatiquement au-delà d'une période d'inactivité définie dans la politique de sécurité de l'établissement ou de l'école.	R	R
INF-PDT-11	Sécurité des données	Si des données administratives sont malgré tout stockées sur le poste de travail des personnels non enseignants (personnels de direction, personnels administratifs…) ou du directeur d'école, ces données doivent être protégées ; elles PEUVENT être chiffrées (chiffrement de masse) et DOIVENT être sauvegardées.	E	E
INF-PDT-12	Accessibilité	Les personnes en situation de handicap DOIVENT être équipées de postes adaptés.	E	E
INF-PDT-13	Accessibilité	Les élèves à besoins éducatifs particuliers DOIVENT pouvoir disposer d'un poste de travail adapté lors des examens.	E	E
INF-PDT-14	Virtualisation	Si elles sont utilisées, les techniques de déport des applications (virtualisation par exemple) DOIVENT tenir compte des contraintes de débit réseau et des impacts sur l'infogérance (gestion des accès, des serveurs de distribution, des impressions…).	E	E
INF-PDT-15	AVEC (BYOD)	Les postes de travail privés des personnels PEUVENT être utilisés dans l'établissement/l'école (BYOD – Bring Your Own Device - ou AVEC en français – Apportez Votre Équipement personnel de Communication). Dans ce cas, la politique de sécurité de l'établissement et le règlement intérieur DEVRAIENT décrire précisément les modalités d'accès ainsi que les limites de responsabilités (ex : assurance, responsabilité juridique vis-à-vis des usages, etc.). Un paragraphe spécifique DEVRAIT également être ajouté à la charte de l'établissement / de l'école (ex : propriété, vie privée, responsabilité juridique vis-à-vis des usages, etc.).	F R	F R

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
INF-PDT-16	Partage	Dans le cas où le poste est partagé entre plusieurs utilisateurs, le service de régénération et de configuration de stations DEVRAIT être activé. Il est nécessaire de définir clairement les procédures de régénération ou de reconfiguration du poste, la qualité de service attendue (notamment au regard du temps), et le traitement réservé aux données locales.	R	R
INF-PDT-17	Partage	Un poste fixe partagé DEVRAIT faire l'objet d'une procédure d'arrêt automatique en fin de journée.	R	R
INF-PDT-18	Partage	Le partage d'un poste de travail PEUT avoir des impacts sur l'organisation. Les règles d'usage et en particulier les droits d'accès au poste sont définies par les équipes pédagogiques.	F	F
INF-PDT-19	Partage	Les utilisateurs DOIVENT être sensibilisés au processus de partage des postes de travail et formés au mécanisme de régénération de configuration et à ses impacts. Cette information DOIT figurer dans la charte de l'établissement/école ou dans les CGU du service.	E	E
INF-PDT-20	Poste en libre-service	Les postes en libre-service DOIVENT être configurés pour ne donner accès qu'à des services non sensibles. Ces postes NE DOIVENT PAS contenir de données personnelles.	E	E

3.2.3 Service d'authentification

Service d'authentification

Du fait de la responsabilité juridique liée à la fourniture d'accès au réseau et à internet ainsi qu'au caractère personnel de certaines données, tout utilisateur DOIT être identifié (voir **service d'annuaire)** et authentifié de façon unique avant d'accéder aux ressources. Cela nécessite la mise en œuvre de mécanismes d'authentification en établissement/école.



Tout utilisateur, et donc tout élève, dispose de moyens d'authentification propres et dont il est responsable.

Impacts sur les infrastructures

L'authentification, parce qu'elle fait partie du processus de contrôle d'accès aux services, DOIT se faire au plus près de l'utilisateur notamment pour permettre l'accès aux ressources locales en toutes circonstances (par exemple, même en cas de coupure internet).

Authentification simple : Tout accès aux ressources, internes ou externes, DOIT être soumis à authentification.

Authentification renforcée : Certains utilisateurs PEUVENT utiliser un moyen d'authentification forte pour accéder à une ressource sensible. Le besoin et la gradation de l'authentification forte DOIVENT être définis en fonction du niveau de criticité (analyse de risques) du service accédé.

Multiplicité des authentifications : Il est important d'appréhender l'authentification de façon unifiée, qu'il s'agisse de l'accès au terminal, de l'accès au réseau local, de l'accès à l'ENT et à ses services tiers* (accès par login/mot de passe), ou de l'accès à d'autres services* dont certains peuvent être des services sensibles (réauthentification ou authentification forte).
**inclut les téléservices*
Le mécanisme d'authentification unique (SSO = Single Sign On) DEVRAIT être mis en oeuvre. Pour les services plus sensibles, deux gradations sont possibles : réauthentification, puis authentification forte. Le SSO DOIT donc préserver la distinction entre authentifications faible et forte en propageant la méthode d'authentification employée.

Postes partagés :Un mécanisme permettant de repérer visuellement et aisément qui est connecté sur le terminal DEVRAIT être présent.

Le service d'authentification DOIT être activé quel que soit le terminal utilisé.

*Pour les terminaux mobiles, se référer au **dossier CARMO**.*

Impacts sur l'organisation

Spécificité 1er degré

L'étape d'authentification peut poser des problèmes de faisabilité pour les plus jeunes élèves du 1er degré. Pour les très jeunes enfants et les non lecteurs, un mode d'authentification simplifié DEVRAIT être envisagé (ex : mise dans l'ordre de 3 ou 4 images).

En maternelle, la conservation d'une liste des moyens d'authentification des enfants par l'enseignant est admissible vu la faible valeur de preuve de l'authentification dans cet environnement.

Dans le cas d'un équipement individuel mobile, des modes de reconnaissance biométriques PEUVENT être utilisés, à la condition que la donnée qui permet la validation de l'accès, soit uniquement stockée dans le terminal et accessible au seul processus d'authentification. [*Note : Les aspects juridiques liés à ces pratiques sont en cours d'instruction*.

L'authentification DEVRAIT être systématique, notamment pour son intérêt pédagogique.

Les chefs d'établissement/directeurs d'école organisent l'attribution des moyens d'authentification aux utilisateurs de leur établissement/école et/ou veillent à leur bonne utilisation.

Les règles de partage des postes des élèves à besoins éducatifs particuliers avec les AVS/AESH DOIVENT être définies dans la charte de l'établissement ou de l'école.

Les administrateurs techniques ont un accès « super utilisateur » sur de nombreux services d'infrastructure. Cela leur donne des droits et des devoirs particuliers qui DOIVENT être formalisés dans une Charte administrateur technique.

Le respect et la bonne gestion d'un service d'authentification (en particulier la gestion des mots de passe) doit s'accompagner d'une sensibilisation des utilisateurs sur leur responsabilité.

Le rythme de changement des mots de passe DOIT être défini dans la politique de sécurité de l'établissement ou de l'école.

Le processus de régénération d'un nouveau mot de passe, en cas d'oubli, DEVRAIT être indiqué dans les conditions d'utilisation des services.

Impacts sur la sécurité des SI

L'authentification simple repose souvent sur la saisie d'un login et d'un mot de passe dont les caractéristiques (longueur et composition) DOIVENT être définies dans la politique de sécurité de l'établissement ou de l'école et rappelées dans les conditions d'utilisation des services.

Le besoin et la gradation de l'authentification forte DOIVENT être définis en fonction du niveau de criticité (analyse de risques) du service accédé.

Une fois distribués aux utilisateurs, les mots de passe DOIVENT être changés dès la première connexion et définis par l'utilisateur.

Les mots de passe ne DOIVENT jamais être stockés en clair que ce soit sous forme numérique ou sur papier.

Le processus de régénération d'un nouveau mot de passe, en cas d'oubli, DOIT être spécifié dans la politique de sécurité de l'établissement ou de l'école. Toute tentative d'authentification, réussie ou échouée, DOIT être tracée, identifiée et horodatée. (voir **service de gestion des journaux).**

Aspects juridiques

Le développement d'Internet a profondément modifié la notion même d'identité. D'une identité classiquement vue comme unique, celle de notre état civil, nous sommes passés aujourd'hui à des identités numériques plurielles. Nous pouvons ici apparaître sous notre « vrai nom », là sous un pseudonyme, un avatar, ici encore sous un simple numéro. Ce développement des identités numériques s'est accompagné rapidement d'une nouvelle forme de fraude : l'usurpation d'identité.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/identites-numeriques-et-usurpation-didentite.html

La CNIL donne des recommandations pour la constitution et la gestion des mots de passe :

https://www.cnil.fr/fr/construire-un-mot-de-passe-sur-et-gerer-la-liste-de-ses-codes-dacces

Interaction avec d'autres services

- ☒ annuaire
- ☒ poste de travail
- ☐ authentification
- ☒ sécurité et accès réseau
- ☐ diffusion d'information
- ☐ sauvegarde
- ☐ régénération de configurations
- ☐ supervision et exploitation
- ☒ gestion des journaux
- ☐ gestion de parc
- ☐ stockage / synchronisation
- ☐ messagerie électronique
- ☐ communication temps réel
- ☐ publication
- ☐ recherche documentaire

INF-AUT Service d'authentification

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
INF-AUT-1	Authentification	Tout utilisateur DOIT être identifié (via le service d'annuaire) et authentifié avant l'accès à toute ressource locale et/ou distante. L'authentification, parce qu'elle fait partie du processus de contrôle d'accès aux services, DOIT se faire au plus près de l'utilisateur notamment pour permettre l'accès aux ressources locales en toutes circonstances. Le service d'authentification DOIT être activé quel que soit le terminal utilisé. *L'étape d'authentification peut poser des problèmes de faisabilité pour les plus jeunes élèves du 1er degré. Pour les très jeunes enfants et les non lecteurs, un mode d'authentification simplifié DOIT être envisagé (ex : mise dans l'ordre de 3 ou 4 images). L'authentification DEVRAIT être systématique, notamment pour son intérêt pédagogique.	R*	E
INF-AUT-2	Authentification forte	Certains utilisateurs PEUVENT utiliser un moyen d'authentification forte pour accéder à une ressource sensible. Le besoin et la gradation de l'authentification forte DOIVENT être définis en fonction du niveau de criticité (analyse de risques) du service accédé.	F	F
INF-AUT-3	Authentification unique (SSO)	Un mécanisme d'authentification unique (SSO = Single Sign On) DEVRAIT être mis en oeuvre. Pour les services plus sensibles, deux gradations sont possibles : réauthentification, puis authentification forte. Le SSO DOIT donc préserver la distinction entre authentifications faible et forte en propageant la méthode d'authentification employée.	R	R
INF-AUT-4	Postes partagés	Un mécanisme permettant de repérer visuellement et aisément qui est connecté sur le terminal DEVRAIT être présent.	R	R
INF-AUT-5	Administrateurs techniques	Les administrateurs techniques ont un accès « super utilisateur » sur de nombreux services d'infrastructure. Cela leur donne des droits et des devoirs particuliers qui DOIVENT être formalisés dans une Charte administrateur technique.	R	R
INF-AUT-6	Mots de passe	L'authentification simple repose souvent sur la saisie d'un login et d'un mot de passe dont les caractéristiques (longueur et composition) DOIVENT être définies dans la politique de sécurité de	E	E

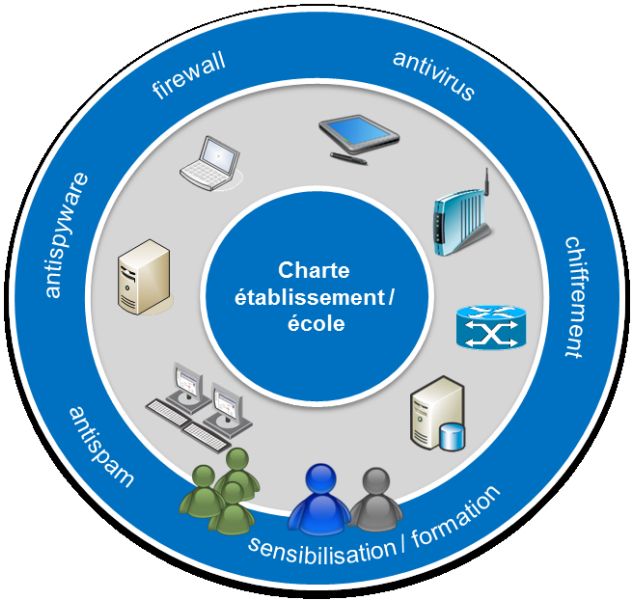
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
		l'établissement ou de l'école et rappelées dans les conditions d'utilisation des services.		
INF-AUT-7	Mots de passe	Une fois distribués aux utilisateurs, les mots de passe DOIVENT être changés dès la première connexion et définis par l'utilisateur.	E	E
INF-AUT-8	Mots de passe	Le rythme de changement des mots de passe DOIT être défini dans la politique de sécurité de l'établissement ou de l'école.	E	E
INF-AUT-9	Mots de passe	Le processus de régénération d'un nouveau mot de passe, en cas d'oubli, DOIT être spécifié dans la politique de sécurité de l'établissement ou de l'école.	E	E
INF-AUT-10	Mots de passe	Les mots de passe ne DOIVENT jamais être stockés en clair que ce soit sous forme numérique ou sur papier. *En maternelle, la conservation d'une liste des moyens d'authentification des enfants par l'enseignant est admissible vu la faible valeur de preuve de l'authentification dans cet environnement.	R*	E
INF-AUT-11	Accessibilité	Les règles de partage des postes des élèves à besoins éducatifs particuliers avec les AVS/AESH DOIVENT être définies dans la charte de l'établissement ou de l'école.	E	E
INF-AUT-12	Biométrie	Dans le cas d'un équipement individuel mobile, des modes de reconnaissance biométriques PEUVENT être utilisés, à la condition que la donnée qui permet la validation de l'accès, soit uniquement stockée dans le terminal et accessible au seul process d'authentification.	F	F
INF-AUT-13	Traçabilité	Toute tentative d'authentification, réussie ou échouée, DOIT être tracée, identifiée et horodatée.	E	E

3.2.4 Service de sécurité et d'accès réseau

Service de sécurisation et d'accès au réseau

L'utilisation des services numériques doit se faire dans des conditions de sécurité optimales dont les principes sont définis dans la PSSI de l'établissement ou de l'école et dans le respect de sa charte.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/charte.html



Ces principes visent simultanément à assurer :

- la sécurité du système d'information de l'établissement ou de l'école :
- celle des systèmes d'information tiers auxquels lui-même donne accès ;
- la protection des mineurs dans le cadre de l'utilisation des outils numériques.

Impacts sur les infrastructures

Le service de sécurisation et d'accès au réseau DOIT permettre :

- de sécuriser les postes de travail, fixes ou nomades ainsi que les serveurs ;

  *Pour les terminaux mobiles, se référer au **dossier CARMO**.*
- de protéger les données ;
- le filtrage des flux entrants et sortants, en particulier le filtrage des sites web et des flux de communication, dans le cadre de la protection de l'élève mineur ;
- que l'accès aux différents réseaux, filaire ou sans fil (pour le Wi-Fi, se reporter au **référentiel Wi-Fi**), en particulier internet, soit réservé aux seuls machines et utilisateurs autorisés (parc de l'établissement et terminaux personnels enregistrés).

La performance de l'accès aux réseaux (intranet, extranet, internet) a un impact sur l'ensemble des services d'infrastructure et plus largement sur l'ensemble des usages numériques. Un accès performant au réseau DOIT donc être une priorité dans tous les plans d'équipement des établissements/écoles. Les capacités du raccordement à internet, des point d'accès Wi-Fi, des équipements de réseau et de sécurité, et du câblage DOIVENT donc être définis en cohérence pour assurer la meilleure performance.

Point d'attention : avec le développement du très haut débit il est nécessaire d'expertiser les performances du réseau interne de l'établissement ou de l'école afin de tirer parti de l'augmentation du débit externe.

Le service de sécurité est un service transverse dont le niveau global est conditionné par celui de son maillon le plus faible. Tous les services d'infrastructure DOIVENT donc prendre en compte la sécurité afin d'assurer la cohérence et la solidité de la chaîne globale.

Impacts sur l'organisation

La sécurité est l'affaire de tous et repose en grande partie sur la bonne compréhension des responsabilités de chacun et donc sur la sensibilisation des acteurs (personnels, élèves, parents, collectivités territoriales, prestataires). Les principes et les règles DEVRAIENT être décrits aux différents niveaux que constituent la politique de sécurité de l'établissement ou de l'école(ex : distribution et réinitialisation des mots de passe), la charte de l'établissement ou de l'école (ex : la non communication de ses moyens d'authentification à des tiers), le règlement intérieur (ex : entrée/sortie des équipements dans l'établissement/école), les conditions générales d'utilisation des équipements (ex : règles de sauvegarde des données situées sur les postes de travail) et/ou dans les contrats de services entre les partenaires (ex : règles d'infogérance).

Filtrage

Les règles de filtrage définies dans les équipements de sécurité, en particulier pour ce qui concerne la protection des mineurs, DOIVENT être sous la responsabilité de l'Éducation nationale/de l'Enseignement agricole.

Il est indispensable de mettre en place à la fois le filtrage des flux et le filtrage de contenu (web, SMTP, etc.) dans le but d'assurer au mieux la protection des mineurs, celle du système d'information et le respect des valeurs du service public de l'éducation (neutralité, etc.)

Toutes les méthodes de filtrage PEUVENT être combinées (listes, analyse de contenu…) ; le service ne saurait reposer uniquement sur des listes d'autorisation, sauf contextes particuliers (très jeunes enfants ? épreuves d'examen ?). Ces contextes et les règles applicables DOIVENT être définis par les équipes pédagogiques, hormis le filtrage des contenus manifestement illicites qui est défini au niveau national.

Le service DOIT permettre l'ajout ou le retrait de règles de filtrage de façon simple et adaptée aux personnes autorisées de l'établissement ou de l'école. Le service DEVRAIT proposer un mécanisme de délégation au plus près de l'acte pédagogique.

Le service DEVRAIT être capable de prendre en compte le groupe classe ou le groupe discipline, et d'une façon plus générale tout groupe pédagogique.

Le service DOIT être en mesure d'utiliser les listes de restrictions et d'autorisations actuellement collectées et maintenues par l'université de Toulouse 1.

Chaîne d'alerte : Une chaîne d'alerte et de responsabilités DOIT être mise en place aux niveaux local et académique pour qualifier, investiguer, traiter les incidents. Chacun a un devoir d'alerte, la détection des incidents DOIT donc être l'affaire de tous.

Impacts sur la sécurité des SI

La performance de l'accès aux réseaux (interne, externe) a un impact sur la disponibilité des services d'infrastructure et plus largement sur l'ensemble des usages numériques.

Il convient de noter que les besoins en débits sont fonction des usages et du nombre de terminaux connectés aux infrastructures de l'EPLE ou de l'école. C'est donc très variable d'un établissement à un autre. La Caisse des dépôts et consignations a effectué des études à ce sujet, notamment en ce qui concerne les écoles :

- http://www.caissedesdepots.fr/sites/default/files/medias/ddnt-usages_numeriques-ecole_Mai_2014.pdf
- http://www.avicca.org/document/14418/dl

Aspects juridiques

Protection des mineurs :

Le service de filtrage de contenu (web, SMTP, etc.) est une obligation réglementaire, rappelée par la circulaire N°2004-035 du 18-2-2004 relative à l'usage de l'internet dans le cadre pédagogique et [à la] protection des mineurs) - http://www.education.gouv.fr/bo/2004/9/MENT0400337C.htm

Consulter régulièrement les textes sur la protection des mineurs :

http://eduscol.education.fr/internet-responsable/ressources/legamedia/protection-des-mineurs.html

Rappelons que le chef d'établissement est responsable du cycle de vie des identités des élèves. C'est également sous sa responsabilité que s'effectuent l'attribution ou la suspension des accès, ainsi que la définition des habilitations liées

à l'usage des services numériques de l'EPLE.

Le chef d'établissement/l'IEN de circonscription est responsable du traitement des données à caractère personnel, des contenus publiés, des usages des services, de la protection des mineurs…

http://www.education.gouv.fr/cid3946/guide-juridique-du-chef-d-etablissement.html

https://www.cnil.fr/fr/traitements-de-gestion-scolaire-quelles-formalites-cnil-pour-les-chefs-detablissements-0

http://eduscol.education.fr/internet-responsable/ressources/legamedia/filtrage.html

Interaction avec d'autres services

☒ annuaire	☒ sauvegarde	☒ stockage / synchronisation
☒ poste de travail	☒ régénération de configurations	☒ messagerie électronique
☒ authentification	☒ supervision et exploitation	☒ communication temps réel
☐ sécurité et accès réseau	☒ gestion des journaux	☒ publication
☒ diffusion d'information	☒ gestion de parc	☒ recherche documentaire

INF-SEC Service de sécurisation et d'accès au réseau

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
INF-SEC-1	Périmètre	Le service de sécurisation et d'accès au réseau DOIT permettre : • de sécuriser les postes de travail, fixes ou nomades, ainsi que les serveurs ; • de protéger les données ; • le filtrage des flux entrants et sortants, en particulier le filtrage des sites web et des flux de communication, dans le cadre de la protection de l'élève mineur ; • que l'accès aux différents réseaux, filaire ou sans fil, en particulier internet, soit réservé aux seuls machines et utilisateurs autorisés (parc de l'établissement et terminaux personnels enregistrés).	E	E
INF-SEC-2	Sécurité réseau	Un accès performant au réseau DOIT être une priorité dans tous les plans d'équipement des établissements/écoles. Les capacités du raccordement à internet, des point d'accès Wi-Fi, des équipements de réseau et de sécurité, et du câblage DOIVENT donc être définis en cohérence pour assurer la meilleure performance.	E	E
INF-SEC-3	Politique de sécurité	La sécurité est l'affaire de tous et repose en grande partie sur la bonne compréhension des responsabilités de chacun et donc sur la sensibilisation des acteurs (personnels, élèves, parents, collectivités territoriales, prestataires). Les principes et les règles DEVRAIENT être décrits aux différents niveaux que constituent la politique de sécurité de l'établissement ou de l'école(ex : distribution et réinitialisation des mots de passe), la charte de l'établissement ou de l'école (ex : la non communication de ses moyens d'authentification à des tiers), le règlement intérieur (ex : entrée/sortie des équipements dans l'établissement/école), les conditions générales d'utilisation des équipements (ex : règles de sauvegarde des données situées sur les postes de travail) et/ou dans les contrats de services entre les partenaires (ex : règles d'infogérance).	R	R

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
INF-SEC-4	Filtrage	Il est indispensable de distinguer le filtrage des flux (niveaux 2 à 4 du modèle OSI), du filtrage de contenu (web, SMTP, etc.) destiné notamment à assurer la protection des mineurs et le respect des valeurs du service public de l'éducation (neutralité, etc.). Toutes les méthodes de filtrage PEUVENT être combinées (listes, analyse de contenu…) ; le service ne saurait reposer uniquement sur des listes d'autorisation, sauf contextes particuliers (très jeunes enfants ? épreuves d'examen ?).	F	F
INF-SEC-5	Filtrage	Les contextes particuliers (très jeunes enfants ? épreuves d'examen ?) et les règles applicables DOIVENT être définis par les équipes pédagogiques, hormis le filtrage des contenus manifestement illicites qui est défini au niveau national.	E	E
INF-SEC-6	Filtrage	Le service DEVRAIT proposer un mécanisme de délégation au plus près de l'acte pédagogique.	R	R
INF-SEC-7	Filtrage	Les règles de filtrage définies dans les équipements de sécurité, en particulier pour ce qui concerne la protection des mineurs, DOIVENT être sous la responsabilité de l'Éducation nationale/de l'Enseignement agricole.	E	E
INF-SEC-8	Filtrage	Le service DOIT pouvoir utiliser les listes de restrictions et d'autorisations actuellement collectées et maintenues par l'université de Toulouse 1.	E	E
INF-SEC-9	Filtrage	Le service DOIT permettre l'ajout ou le retrait de règles de filtrage par les personnes autorisées de l'établissement ou de l'école.	E	E
INF-SEC-10	Filtrage	Le service DEVRAIT être capable de prendre en compte le groupe classe ou le groupe discipline, et d'une façon plus générale tout groupe pédagogique.	R	R

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
INF-SEC-11	Chaîne d'alerte	Une chaîne d'alerte et de responsabilités DOIT être mise en place aux niveaux local et académique pour qualifier, investiguer, traiter les incidents. Chacun a un devoir d'alerte, la détection des incidents DOIT donc être l'affaire de tous.	E	E
INF-SEC-12	Tous les services	Le service DEVRAIT permettre une administration et une exploitation de la sécurité des services (à ne pas confondre avec la gestion des règles de filtrage) centralisées.	R	R

3.2.5 Service de diffusion d'information

Service de diffusion d'information

Ce service a pour objet de permettre la diffusion de messages (horaires, absences, menus, actualités…) sur des écrans installés dans des espaces publics ou communs de l'établissement ou de l'école (hall d'accueil, circulations, salle des professeurs…).

Impacts sur les infrastructures

Le service de diffusion fournit les infrastructures matérielles et logicielles nécessaires pour saisir, modifier, diffuser, supprimer des messages sur des écrans installés dans des espaces publics ou communs.

Le service PEUT diffuser le même contenu sur tous les écrans, sur plusieurs écrans ou diffuser un contenu différent selon les écrans. Le service PEUT proposer du multifenêtrage (plusieurs flux de contenus sur le même écran).

Le service PEUT proposer la programmation de la diffusion à des horaires prédéfinis. Il DEVRAIT être possible d'interrompre la diffusion en cours pour la diffusion de message à caractère d'urgence, sans perte du contenu initial.

Les contenus PEUVENT provenir du service de publication et le service DEVRAIT faciliter cette interopérabilité. (voir **service de publication).**

Connectique : Ces équipements DEVRAIENT utiliser les mêmes infrastructures matérielles réseau (câblage, actifs de réseau…) que les autres équipements (serveurs de fichiers, etc.) de l'établissement/école.

Accès : L'accès DOIT être sécurisé et strictement réservé au personnel depuis un poste situé en zone « administrative », ou depuis le poste du directeur d'école. Le système DEVRAIT pour cela permettre d'identifier les panneaux d'affichage.

Le service PEUT proposer la reprise automatique de données sur des applications tiers proposant des exports automatiques (ex. flux RSS, réservation de ressources, etc.).

Sauvegarde : Les contenus diffusés DEVRAIENT être sauvegardés et archivés. (voir **service sauvegarde**).

Impacts sur l'organisation

Les droits d'accès au service DOIVENT être attribués par le chef d'établissement/directeur d'école/IEN de circonscription en tant que responsable de la publication.

Impacts sur la sécurité des SI

Le service ne DOIT être accessible que depuis des postes sécurisés et localisés dans la zone « administrative » et PEUT être protégé par authentification forte.

Toute diffusion de message DEVRAIT être tracée, identifiée et horodatée. (voir **service de gestion des journaux)**

Aspects juridiques

Articles à consulter :

http://eduscol.education.fr/internet-responsable/ressources/legamedia/liberte-d-expression-et-ses-limites.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/image-et-video.html

Interaction avec d'autres services

☐ annuaire	☒ sauvegarde	☐ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☒ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☒ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

INF-DIF Service de diffusion d'information

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
INF-DIF-1	Accès	L'accès DOIT être sécurisé et strictement réservé au personnel depuis un poste situé en zone « administrative », ou depuis le poste du directeur d'école.	E	E
INF-DIF-2	Accès	Le système DEVRAIT pour cela permettre d'identifier les panneaux d'affichage.	R	R
INF-DIF-3	Accès	Le service PEUT proposer la reprise automatique de données sur des applications tiers proposant des exports automatiques (ex. flux RSS, réservation de ressources, etc.).	F	F
INF-DIF-4	Accès	L'accès aux outils d'édition et de diffusion PEUT être soumis à authentification forte.	F	F
INF-DIF-5	Accès	Les droits d'accès au service DOIVENT être attribués par le chef d'établissement/directeur d'école en tant que responsable de la publication.	E	E
INF-DIF-6	Diffusion	Le service PEUT diffuser le même contenu sur tous les écrans, sur plusieurs écrans ou diffuser un contenu différent selon les écrans.	F	F
INF-DIF-7	Diffusion	Le service PEUT proposer du multifenêtrage (plusieurs flux de contenus sur le même écran).	F	F
INF-DIF-8	Diffusion	Le service PEUT proposer la programmation de la diffusion à des horaires prédéfinis	F	F
INF-DIF-9	Diffusion	Il DEVRAIT être possible d'interrompre la diffusion en cours pour la diffusion de message à caractère d'urgence, sans perte du contenu initial.	R	R
INF-DIF-10	Contenus	Les contenus PEUVENT provenir du service de publication et le service DEVRAIT faciliter cette interopérabilité	F	F

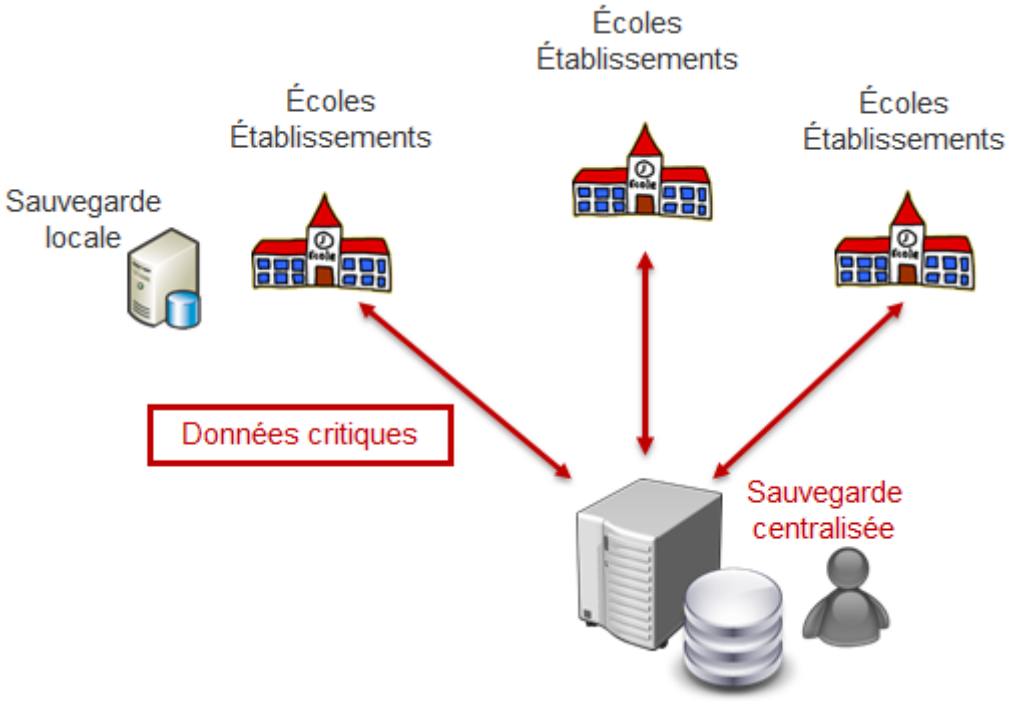
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
INF-DIF-11	Connectique	Le service DEVRAIT utiliser les mêmes infrastructures matérielles réseau (câblage, actifs de réseau…) que les autres équipements (serveurs de fichiers, etc.) de l'établissement/école.	R	R
INF-DIF-12	Sauvegarde/Archivage	Les contenus diffusés DEVRAIENT être sauvegardés et archivés.	R	R
INF-DIF-13	Traçabilité	Toute diffusion de message DEVRAIT être tracée, identifiée et horodatée.	R	R

3.3 Services de maintien en condition opérationnelle

3.3.1 Service de sauvegarde

Service de sauvegarde

Garantir la qualité de service passe par la préservation des données et la capacité de restaurer sur demande ces données.



Le service de sauvegarde offre les mécanismes et les procédures (fréquences, volumes, supports, lieux de stockage…) permettant de sauvegarder et de restaurer les données des utilisateurs et les données techniques sensibles.

Impacts sur les infrastructures

Les solutions de sauvegarde DOIVENT exister. Une solution centralisée DEVRAIT être mise en œuvre chaque fois que les usages et les débits le permettent.

Le service de sauvegarde DEVRAIT permettre de conserver/restaurer plusieurs versions de données sauvegardées.

Certaines données font l'objet d'un cadre juridique précis quant à leur durée et conditions de rétention (journaux d'accès à internet, données comptables, données de vie scolaire, données de santé, examens et concours…). La capacité du service doit permettre de répondre aux durées légales de conservation de ces données. (voir **service de gestion des journaux**).

Voir les instructions de tri et de conservation des archives concernant l'Éducation nationale.

ftp://trf.education.gouv.fr/pub/edutel/bo/2005/24/tableaux_encart24.pdf

*Pour la sauvegarde des données stockées sur les terminaux mobiles, se référer au **dossier CARMO.***

Impacts sur l'organisation

Le service de sauvegarde DOIT permettre de planifier les sauvegardes selon une politique qui définit :

- un échéancier (fréquence et calendrier),
- les critères de sélection des données à sauvegarder (arborescences, noms, extensions, dates, versions…),
- les types de sauvegardes (incrémentale, différentielle, sélective, complète).

Les procédures et mécanismes de restauration de données sauvegardées DEVRAIENT être testés régulièrement. Le rythme de ces tests DEVRAIT figurer dans les clauses contractuelles ou les CGU du service.

Les utilisateurs DOIVENT être informés (charte d'établissement/école) de la durée de conservation de leurs données et de la procédure de restauration.

Le service de sauvegarde PEUT permettre l'extraction des supports de sauvegarde de telle sorte qu'ils soient stockés dans un site distant du site de production du support.

L'utilisateur doit être informé du fait que le choix du lieu de stockage de ses données a des impacts sur la sauvegarde de ses données. Cette information DOIT figurer dans la charte et/ou dans les CGU du service.

Par exemple :

- dans l'ENT ou sur les serveurs de l'établissement – données sauvegardées par le service;
- sur le disque du poste de travail – selon politique de sauvegarde de l'établissement/école,
- ailleurs (clés USB, disques externes, dans le cloud…) – données sauvegardées par l'utilisateur.

Les administrateurs techniques des sauvegardes ne DOIVENT pas accéder au contenu des sauvegardes (sauf accord de l'utilisateur ou sur demande d'une autorité judiciaire).

Impacts sur la sécurité des SI

Le service de sauvegarde est essentiel pour garantir l'intégrité et la disponibilité des données et peut avoir des conséquences sur la confidentialité.

Ces trois critères (intégrité, confidentialité et disponibilité) sont à considérer ensemble. Par exemple, transférer des données de l'environnement professionnel vers l'environnement grand public peut répondre au critère de disponibilité mais porter gravement atteinte à la confidentialité.

Le choix de l'emplacement physique du stockage des sauvegardes doit prendre en compte l'éventualité d'un sinistre. Un premier niveau de sécurité peut être apporté par l'éloignement physique au sein de l'établissement des stockages des données sauvegardées. En complément, le stockage des données DEVRAIT être éloigné physiquement du stockage des sauvegardes. Une sensibilisation particulière DOIT donc être programmée sur ce sujet.

Si des données administratives sont stockées sur le poste de travail des personnels non enseignants (personnels de direction, personnels administratifs…) ou du directeur d'école, ces données doivent être protégées ; Elles PEUVENT être chiffrées (chiffrement de masse) et DOIVENT être sauvegardées (voir **service Poste de travail** et **service de stockage)**.

Les flux des données à sauvegarder/restaurer DOIVENT être sécurisés (confidentialité et intégrité).

Aspects juridiques

Articles à consulter :

http://eduscol.education.fr/internet-responsable/ressources/legamedia/donnees-personnelles-et-obligation-de-securite.html

Interaction avec d'autres services

☐ annuaire	☐ sauvegarde	☒ stockage / synchronisation
☒ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

MCO-SVG Service de sauvegarde

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
MCO-SVG-1	Sauvegarde / Restauration	Le service de sauvegarde DOIT offrir les mécanismes et les procédures (fréquences, volumes, supports, lieux de stockage…) permettant de sauvegarder et de restaurer les données des utilisateurs et les données techniques sensibles.	E	E
MCO-SVG-2	Planification	Le service de sauvegarde DOIT permettre de planifier les sauvegardes selon une politique qui définit : • un échéancier (fréquence et calendrier), • les critères de sélection des données à sauvegarder (arborescences, noms, extensions, dates, versions…), • les types de sauvegardes (incrémentale, différentielle, sélective, complète).	E	E
MCO-SVG-3	Historisation	Le service de sauvegarde DEVRAIT permettre de conserver/restaurer plusieurs versions de données sauvegardées.	R	R
MCO-SVG-4	Supports	Le service de sauvegarde PEUT permettre l'extraction des supports de sauvegarde de telle sorte qu'ils soient stockés dans un site distant du site de production du support.	F	F
MCO-SVG-5	Supports	Le choix de l'emplacement physique du stockage des sauvegardes doit prendre en compte l'éventualité d'un sinistre. Le stockage des données DEVRAIT être éloigné physiquement du stockage des sauvegardes.	R	R
MCO-SVG-6	Administration technique	Les solutions de sauvegarde centralisée DEVRAIENT être mises en œuvre chaque fois que les usages et les débits le permettent.	R	R

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
MCO-SVG-7	Sauvegarde des données locales	Il est déconseillé de stocker des données sur le poste de travail, a fortiori des données administratives. Si des données administratives sont malgré tout stockées sur le poste de travail des personnels non enseignants (personnels de direction, personnels administratifs…) ou du directeur d'école, ces données doivent être protégées ; Elles PEUVENT être chiffrées (chiffrement de masse) et DOIVENT être sauvegardées.	E	E
MCO-SVG-8	Restauration	Les procédures et mécanismes de restauration de données sauvegardées DEVRAIENT être testés régulièrement. Le rythme de ces tests DEVRAIT figurer dans les clauses contractuelles ou les CGU du service.	E	E
MCO-SVG-9	Formation/Sensibilisation	Les utilisateurs DOIVENT être informés (charte d'établissement/école) de la durée de conservation de leurs données et de la procédure de restauration.	E	E
MCO-SVG-10	Formation/Sensibilisation	L'utilisateur doit être informé du fait que le choix du lieu de stockage de ses données a des impacts sur la sauvegarde de ses données. Cette information DOIT figurer dans la charte et/ou dans les CGU du service.	E	E
MCO-SVG-11	Charte administrateur technique	Les administrateurs techniques des sauvegardes ne DOIVENT pas accéder au contenu des sauvegardes (sauf accord de l'utilisateur ou sur demande d'une autorité judiciaire).	E	E
MCO-SVG-12	Transferts	Les flux des données à sauvegarder/restaurer DOIVENT être sécurisés (confidentialité et intégrité).	E	E
MCO-SVG-13	Traçabilité	Chaque sauvegarde/restauration DOIT être tracée, identifiée et horodatée.	E	E

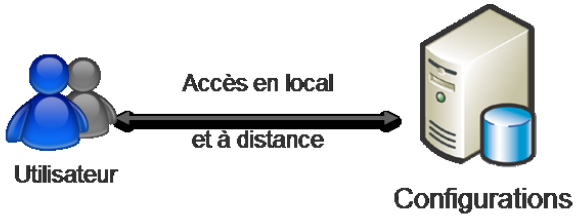
3.3.2 Service de régénération et de configuration de stations

service de régénération et de configuration de stations

En établissement/école, les postes de travail ne sont généralement pas dédiés à un seul utilisateur ou à une seule catégorie d'utilisateurs.

La mise en place d'un service de régénération et de configuration de stations garantit à l'utilisateur qu'il retrouvera un poste fonctionnel ainsi qu'un environnement de travail adapté à son usage.

Le service PEUT permettre également de choisir, lors du démarrage (boot) de la station, la configuration de la station (par exemple, dans le cas du partage de la station entre différents types d'enseignement).



La fonctionnalité attendue consiste donc à pouvoir régénérer une configuration. La finalité peut varier:

- redéploiement de poste ;
- régénération uniquement de profil utilisateurs ;
- régénération de configuration par "discipline" ;
- ...

Il convient de distinguer deux processus distincts :

- la fabrication du « master » : qui consiste à préparer le modèle de la machine vierge (système d'exploitation, pilotes et leurs correctifs respectifs) ;
- le déploiement des applications.

Impacts sur les infrastructures

Le service offre les mécanismes et les procédures permettant de régénérer (automatiquement ou selon nécessité) la configuration d'une station de travail pour un utilisateur ou un groupe d'utilisateurs.

Le service DEVRAIT permettre de sauvegarder et d'activer différentes configurations d'utilisation d'une station de travail (ergonomie, configuration système, bureau…). L'impact du service sur les performances réseau doit être anticipé.

Les mises à jour de sécurité du système et des applications locales DOIVENT être intégrées aux configurations sauvegardées, ainsi que la mise à jour des pilotes matériels des périphériques adaptés aux élèves à besoins éducatifs particuliers.

La régénération de la configuration DEVRAIT être activable en local et à distance, sous réserve de débits réseaux suffisants.

Une fois lancée, la régénération de la configuration DOIT être un processus automatisé.

Pour la régénération et la configuration des terminaux mobiles, se référer au ***dossier CARMO*** *.*

Impacts sur l'organisation

Les règles d'usage du service et en particulier les droits d'accès aux différentes configurations du poste sont définies par les équipes pédagogiques et administratives et DOIVENT être décrites dans les CGU du service.

Les utilisateurs doivent être sensibilisés au processus de partage des postes de travail et formés au mécanisme de régénération de configuration et à ses impacts (performance réseau).

Ils doivent être informés qu'un usage excessif de ce service peut avoir des conséquences sur les performances générales du réseau. Cette information DOIT figurer dans la charte de l'établissement/école ou dans les CGU du

service.

Impacts sur la sécurité des SI

Le service de reconfiguration des configurations est un service essentiel pour garantir la disponibilité des postes de travail.

Ce service est souvent utilisé par les infogérants (dont les prestataires). Les règles d'accès et d'usage au service DOIVENT donc être précisées dans les CGU du service.

La régénération d'une station peut poser des problèmes de sécurité de deux sortes concernant les données des utilisateurs :

- faire disparaître des données personnelles des utilisateurs (risque d'atteinte à l'intégrité) ;
- ou faire réapparaître des données confidentielles qui avaient été effacées (risque d'atteinte à la confidentialité).

Ces risques doivent être gérés avec attention dans la mise en œuvre du service.

Aspects juridiques

Les risques d'atteinte aux données personnelles des utilisateurs (intégrité, confidentialité) doivent être évalués afin d'être minimisés autant que possible. Les utilisateurs doivent être informés de manière formelle (charte ou CGU) des risques résiduels afin qu'ils puissent prendre les mesures adéquates pour leurs données en fonction de leur importance ou de leur sensibilité.

Les contrats avec les sociétés intervenant éventuellement sur ce service doivent également comporter les mentions propres à garantir intégrité et confidentialité de ces données.

Interaction avec d'autres services

☐ annuaire	☒ sauvegarde	☐ stockage / synchronisation
☒ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☒ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

MCO-REG Service de régénération et de configuration de stations

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
MCO-REG-1	Fonctionnalité	Le service DEVRAIT permettre de sauvegarder et d'activer différentes configurations d'utilisation d'une station de travail (ergonomie, configuration système, bureau…).	R	R
MCO-REG-2	Démarrage	Le service PEUT permettre de choisir, lors du démarrage (boot) de la station, la configuration de la station (par exemple, dans le cas du partage de la station entre différents types d'enseignement).	F	F
MCO-REG-3	Mise à jour	Les mises à jour de sécurité du système et des applications locales DOIVENT être intégrées aux configurations sauvegardées, ainsi que la mise à jour des pilotes matériels des périphériques adaptés aux élèves à besoins éducatifs particuliers.	E	E
MCO-REG-4	Activation	La régénération de la configuration DEVRAIT être activable en local et à distance, sous réserve de débits réseaux suffisants.	R	R
MCO-REG-5	Automatisation	Une fois lancée, la régénération de la configuration DOIT être un processus automatisé.	E	E
MCO-REG-6	Architecture	Le service PEUT, pour faciliter la gestion centralisée (stockage des configurations), être réparti entre une partie cliente et une partie serveur.	F	F
MCO-REG-7	Accès	Les règles d'usage du service et en particulier les droits d'accès aux différentes configurations du poste sont définies par les équipes pédagogiques et administratives et DOIVENT être décrites dans les CGU du service.	E	E
MCO-REG-8	Formation/Sensibilisation	Ils doivent être informés qu'un usage excessif de ce service peut avoir des conséquences sur les performances générales du réseau. Cette information DOIT figurer dans la charte de l'établissement/école ou dans les CGU du service.	E	E

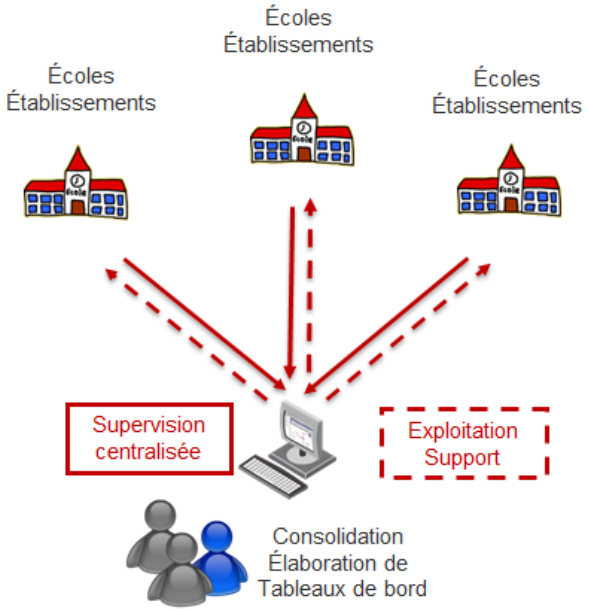
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
MCO-REG-9	CGU	Ce service est souvent utilisé par les infogérants (dont les prestataires). Les règles d'accès et d'usage au service DOIVENT donc être précisées dans les CGU du service.	E	E

3.3.3 Service de supervision et d'exploitation de l'infrastructure

Service de supervision et d'exploitation de l'infrastructure

Le service répond à deux catégories de besoins :

- Garantir la qualité du service rendu par la mise en place d'une organisation, de procédures et d'outils de supervision et d'exploitation des infrastructures en établissement/école,
- Obtenir des statistiques sur l'utilisation des services d'infrastructure.



Impacts sur les infrastructures

La qualité de service attendue suppose la mise en œuvre d'un « service d'exploitation » (au sens du référentiel ITIL® (Information Technology Infrastructure Library)).

Collecter et analyser les événements : Le service DOIT fournir en temps réel un état du fonctionnement des services. Les données remontées (alertes, indicateurs…) peuvent concerner l'ensemble des services d'infrastructure de l'établissement ou de l'école (disponibilité des équipements et des services d'infrastructure, taux d'occupation des espaces disques, occupation de la bande passante réseau, taux d'utilisation des services…). Il est donc important d'être attentif aux impacts sur les espaces de stockage et la bande passante nécessaires.

Gérer les incidents et les problèmes : Le service DOIT fournir les mécanismes permettant de détecter et analyser les incidents afin de restaurer les conditions opérationnelles d'un service en un temps compatible avec les attentes des utilisateurs, définies dans les CGU.

Collecter les demandes des utilisateurs : Le service DOIT fournir une organisation et les mécanismes permettant de collecter et analyser les demandes des utilisateurs afin d'y apporter une réponse adaptée.

Administration technique du service: L'accès à l'administration technique du service DEVRAIT pouvoir être effectué à distance et centralisé. Un mécanisme de prise en main à distance PEUT être utilisé pour la faciliter.

Tableaux de bord : Le service DOIT fournir les outils permettant de construire des tableaux de bord à partir des données remontées des infrastructures supervisées.

*Pour la supervision et l'exploitation des terminaux mobiles, se référer au **dossier CARMO**.*

Impacts sur l'organisation

Il existe des besoins de tableaux de bord pour le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école et chacun DOIT pouvoir disposer des données dont il a besoin pour assurer sa mission. Donc il convient que chacun soit attentif à la diffusion des données dont il dispose.

Le service DOIT fournir aux chefs d'établissement/directeurs d'école le(s) tableau(x) de bord dont ils ont besoin, en

particulier les éléments nécessaires au pilotage de l'établissement/école et au renseignement des enquêtes. En complément, il peut éventuellement leur fournir les données brutes.

Ces éléments peuvent provenir des informations stockées dans les journaux (voir **service de gestion des journaux)** ou du service de gestion de parc (voir **service de gestion de parc)**

Les administrateurs techniques doivent respecter des règles strictes pour l'accès au contenu des données collectées quand elles ont un caractère personnel ou privé (données concernant des personnes identifiées ou identifiables ou encore données appartenant en personne ou en privé à un utilisateur). Les garanties données aux utilisateurs quant aux données les concernant DOIVENT figurer dans la charte de l'établissement/école.

Ces règles DOIVENT être définies dans une charte des administrateurs techniques.

Impacts sur la sécurité des SI

L'accès aux données collectées DOIT être réservé strictement aux personnes autorisées et DEVRAIT être soumis à authentification forte. L'attribution des autorisations est de la responsabilité du chef d'établissement/IEN de circonscription. (voir **service d'authentification**).

Aspects juridiques

Pour des raisons de confidentialité, les données remontées par le service de supervision DEVRAIENT être anonymisées (par exemple via des mécanismes d'agrégation ou de calculs statistiques). Dans l'hypothèse où elles ne le seraient pas, les formalités nécessaires doivent être accomplies auprès de la CNIL et les utilisateurs informés du traitement et de leurs droits.

Interaction avec d'autres services

☐ annuaire	☐ sauvegarde	☐ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☒ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☐ publication
☐ diffusion d'information	☒ gestion de parc	☐ recherche documentaire

MCO-SEI Service de supervision

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
MCO-SEI-1	Collecte des données	Le service DOIT fournir en temps réel un état du fonctionnement des services. Les données remontées (alertes, indicateurs…) peuvent concerner l'ensemble des services d'infrastructure de l'établissement ou de l'école (disponibilité des équipements et des services d'infrastructure, taux d'occupation des espaces disques, occupation de la bande passante réseau, taux d'utilisation des services…). Il est donc important d'être attentif aux impacts sur les espaces de stockage et la bande passante nécessaires.	E	E
MCO-SEI-2	Gestion des incidents	Le service DOIT fournir les mécanismes permettant de détecter et analyser les incidents afin de restaurer les conditions opérationnelles d'un service en un temps compatible avec les attentes des utilisateurs, définies dans les CGU.	E	E
MCO-SEI-3	Gestion des demandes des utilisateurs	Le service DOIT fournir une organisation et les mécanismes permettant de collecter et analyser les demandes des utilisateurs afin d'y apporter une réponse adaptée.	E	E
MCO-SEI-4	Prise en main à distance	L'accès à l'administration technique du service DEVRAIT pouvoir être effectué à distance et centralisé. Un mécanisme de prise en main à distance PEUT être utilisé pour la faciliter.	R	R
MCO-SEI-5	Tableaux de bord	Le service DOIT fournir les outils permettant de construire des tableaux de bord à partir des données remontées des infrastructures supervisées.	E	E
MCO-SEI-6	Tableaux de bord	Il existe des besoins de tableaux de bord pour le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école et chacun DOIT pouvoir disposer des données dont il a besoin pour assurer sa mission. Donc il convient que chacun soit attentif à la diffusion des données dont il dispose. Le service DOIT fournir aux chefs d'établissement/directeurs d'école le(s) tableau(x) de bord dont ils ont besoin, en particulier les éléments nécessaires au pilotage de l'établissement/école et au renseignement des enquêtes.	E	E

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
MCO-SEI-7	Administration technique	Les administrateurs techniques doivent respecter des règles strictes pour l'accès au contenu des données collectées quand elles ont un caractère personnel ou privé (données concernant des personnes identifiées ou identifiables ou encore données appartenant en personne ou en privé à un utilisateur). Les garanties données aux utilisateurs quant aux données les concernant DOIVENT figurer dans la charte de l'établissement/école. Ces règles DOIVENT être définies dans une charte des administrateurs techniques.	E	E
MCO-SEI-8	Anonymisation	Pour des raisons de confidentialité, les données remontées DEVRAIENT être anonymisées (par exemple via des mécanismes d'agrégation ou de calculs statistiques). Dans l'hypothèse où elles ne le seraient pas, les formalités nécessaires doivent être accomplies auprès de la CNIL et les utilisateurs informés du traitement et de leurs droits.	R	R
MCO-SEI-9	Accès	L'accès aux données collectées DOIT être réservé strictement aux personnes autorisées. L'attribution des autorisations est de la responsabilité du chef d'établissement/IEN de circonscription.	E	E
MCO-SEI-10	Accès	L'accès aux données collectées DEVRAIT être soumis à authentification forte.	R	R

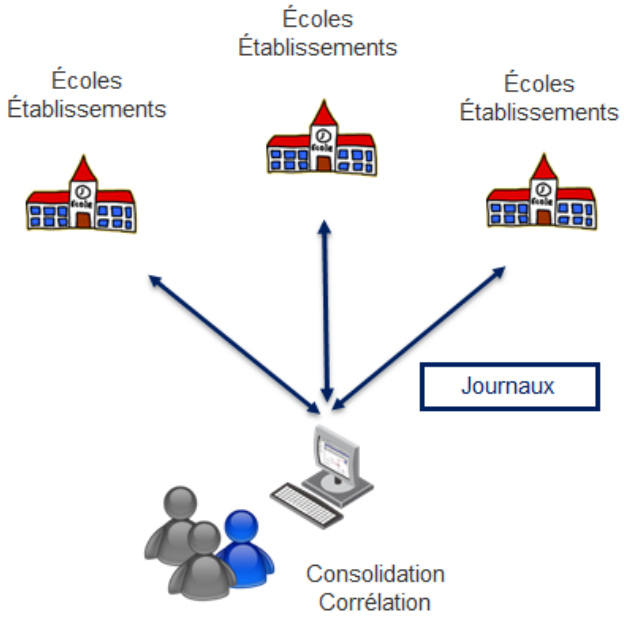
3.3.4 Service de gestion des journaux

Service de gestion des journaux

Le cadre législatif et réglementaire impose des règles en termes de traçabilité.

Les événements tracés sont enregistrés dans des journaux (ou logs).

Ces journaux sont également utiles à des fins de supervision et d'exploitation. (voir **service de supervision et d'exploitation)**



Impacts sur les infrastructures

Les équipements générateurs de journaux DEVRAIENT respecter un format standard et commun de description d'événement.

Le service de gestion des journaux doit prévoir et décrire des procédures et mécanismes d'extraction automatique vers un format qui facilite la consolidation des journaux dans un objectif de supervision centralisée. (voir **service de supervision et d'exploitation)**

Le service de gestion des journaux devrait offrir des mécanismes facilitant son exploitation (compression, archivage, purge,…).

Les équipements d'infrastructure peuvent être « bavards » et le stockage des journaux nécessite souvent un espace disque conséquent. La capacité du service DOIT permettre de répondre aux durées légales de conservation des données.

Le service PEUT compléter les capacités de stockage en ligne avec des mesures d'archivage sur support externe afin de répondre à cette exigence.

*Pour la gestion des journaux des terminaux mobiles, se référer au **dossier CARMO**.*

Impacts sur l'organisation

Le service de gestion des journaux constitue un service de traitement de données à caractère personnel. Les utilisateurs DOIVENT être informés (charte d'établissement/école) des durées de conservation des journaux lorsque ces derniers concernent des données à caractère personnel (journaux de l'ENT, journaux des pare-feu et des dispositifs de filtrage, journaux de connexion au Wi-Fi, journaux système par exemple).

Les besoins de consultation des journaux (quoi, par qui, à quelles fréquences, pour quel objectif …) PEUVENT être définis par le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs

d'école. (voir **service de supervision et d'exploitation)**

Les administrateurs techniques ont un accès technique aux journaux. La consultation du contenu des journaux quand ils contiennent des données à caractère personnel doit être encadrée par des règles, sauf accord de l'utilisateur ou demande d'une autorité judiciaire; ces dernières DOIVENT être définies dans la politique de sécurité de l'établissement/école et dans une charte des administrateurs techniques.

Impacts sur la sécurité des SI

L'accès au service de gestion des journaux DOIT être strictement réservé aux administrateurs techniques. Ce service pouvant comporter des données sensibles, il DEVRAIT être soumis à authentification forte ou substantielle. (voir **service d'authentification)**

En cas de centralisation de tout ou partie de la gestion des journaux, les flux entre les infrastructures de l'établissement/école et le lieu où les données sont centralisées DOIVENT garantir la confidentialité et l'intégrité des données.

Aspects juridiques

Rappelons que le chef d'établissement est responsable de la sécurité des biens et des personnes de l'EPLE, selon le code de l'éducation[1]. Il doit donc s'assurer, en liaison avec les autorités administratives compétentes, que les obligations réglementaires en matière de journaux de sécurité seront respectées.

Dès lors que certains journaux permettent d'identifier directement ou indirectement des personnes physiques, au besoin en les croisant avec toutes données dont dispose le responsable du traitement ou toute autre personne (par exemple l'administrateur système), le système de traitement des journaux constitue un traitement de données à caractère personnel au sens de la loi du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés.

http://eduscol.education.fr/internet-responsable/les-tic-et-lecole/maitriser-lusage-des-reseaux/tracage-vie-privee-et-traitement-des-journaux-informatiques.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/le-droit-a-loubli.html

Interaction avec d'autres services

☐ annuaire	☐ sauvegarde	☐ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☒ authentification	☒ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

1 Code de l'éducation article R421-10

MCO-JAL Service de gestion des journaux

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
MCO-JAL-1	Contenu	Les équipements générateurs de journaux DEVRAIENT respecter un format standard et commun de description d'événement.	R	R
MCO-JAL-2	Capacité	Les équipements d'infrastructure peuvent être « bavards » et le stockage des journaux nécessite souvent un espace disque conséquent. La capacité du service DOIT permettre de répondre aux durées légales de conservation des données.	E	E
MCO-JAL-3	Capacité	Le service PEUT compléter les capacités de stockage en ligne avec des mesures d'archivage sur support externe afin de répondre à cette exigence.	F	F
MCO-JAL-4	Formation/Sensibilisation	Le service de gestion des journaux constitue un service de traitement de données à caractère personnel. Les utilisateurs DOIVENT être informés (charte d'établissement/école) des durées de conservation des journaux lorsque ces derniers concernent des données à caractère personnel (journaux de l'ENT, journaux des pare-feu et des dispositifs de filtrage, journaux de connexion au Wi-Fi, journaux système par exemple).	E	E
MCO-JAL-5	Consultation	Les besoins de consultation des journaux (quoi, par qui, à quelles fréquences, pour quel objectif …) PEUVENT être définis par le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école.	F	F
MCO-JAL-6	Accès	Les administrateurs techniques ont un accès technique aux journaux. La consultation du contenu des journaux quand ils contiennent des données à caractère personnel doit être encadrée par des règles, sauf accord de l'utilisateur ou demande d'une autorité judiciaire; ces dernières DOIVENT être définies dans la politique de sécurité de l'établissement/école et dans une charte des administrateurs techniques.	E	E

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
MCO-JAL-7	Accès	L'accès au service de gestion des journaux DOIT être strictement réservé aux administrateurs techniques. Ce service pouvant comporter des données sensibles, il DEVRAIT être soumis à authentification forte ou substantielle.	E	E
MCO-JAL-8	Flux	En cas de centralisation de tout ou partie de la gestion des journaux, les flux entre les infrastructures de l'établissement/école et le lieu où les données sont centralisées DOIVENT garantir la confidentialité et l'intégrité des données.	E	E

3.3.5 Service de gestion de parc

Service de gestion de parc

Le chef d'établissement / gestionnaire de l'établissement / directeur d'école a besoin de disposer d'un inventaire précis et à jour, facilitant ainsi le suivi du maintien en condition opérationnelle et la réponse aux enquêtes (ETIC, OPINEE…). Le service répond donc à trois catégories de besoins:

- Garantir la maîtrise du parc informatique (matériel + services d'infrastructure) disponible en établissement/école,
- Obtenir des statistiques sur les données de ce parc,
- Faciliter de ce fait la réponse aux enquêtes (ETIC, OPINEE…).

Le service de gestion de parc DOIT fournir, par établissement ou école, un dispositif permettant la gestion de l'inventaire des matériels (postes de travail, serveurs, écrans, vidéo projecteurs, TNI, VNI, appareils photos, équipements réseau et de sécurité, casques audio, caméras, imprimantes, microscopes…). Il DOIT permettre la recherche et les statistiques.

Le service DEVRAIT permettre :

- la catégorisation de ces matériels (fournisseurs, caractéristiques, vétusté, localisation, utilisation…),
- la gestion de la valeur (TCO) et des critères de remplacement et de mise au rebut.
- la gestion du cycle de vie et la planification du remplacement des équipements,
- l'interfaçage avec le service de supervision (en particulier la gestion des incidents).

Le service DEVRAIT permettre la réservation de matériel et PEUT permettre le prêt de matériel.

Le service PEUT intégrer la fonction de gestion du parc applicatif.

*Pour la gestion du parc des terminaux mobiles, se référer au **dossier CARMO**.*

Impacts sur les infrastructures

Le service de gestion de parc DEVRAIT intégrer un mécanisme de découverte automatique des matériels connectés au réseau de l'établissement ou de l'école. Cela nécessite l'installation d'un agent sur les matériels de l'établissement ou de l'école, et cette recommandation devrait être prise en compte dans le choix des équipements.

Les matériels hors parc (BYOD, visiteurs, prestataires…) connectés au réseau DEVRAIENT pouvoir être détectés afin de mesurer l'impact potentiel sur les infrastructures et leur sécurité.

Impacts sur l'organisation

Il existe des besoins de tableaux de bord concernant le matériel pour le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école. Le service DOIT fournir aux chefs d'établissement/directeurs d'école le(s) tableau(x) de bord dont ils ont besoin, en particulier les éléments nécessaires

au pilotage de l'établissement/école et au renseignement des enquêtes. (voir **service de supervision et d'exploitation)**

Impacts sur la sécurité des SI

La gestion de parc constitue un apport important sur la sécurité, en particulier pour la gestion des incidents. Disposer d'un inventaire précis et à jour facilite le maintien en condition opérationnelle.

Une attention particulière doit être portée aux équipements hors parc (BYOD, visiteurs, prestataires…). On PEUT notamment leur appliquer des conditions spécifiques de raccordement au réseau de l'établissement ou de l'école.

Aspects juridiques

La gestion des déchets (dont la mise au rebut des matériels) est régie par le code de l'environnement, publié pour sa partie législative en annexe de l'Ordonnance n° 2000-914 du 18 septembre 2000 (JO du 21 septembre 2000).

La mise au rebut des matériels DOIT respecter la réglementation, en termes d'environnement et d'éventuelle cession de propriété (recyclage interne, dons (écoles, associations…), vente des domaines, sociétés privées de recyclage…).

Interaction avec d'autres services

☐ annuaire	☐ sauvegarde	☐ stockage / synchronisation
☒ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☒ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

MCO-PAR Service de gestion de parc

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
MCO-PAR-1	Fonctionnalités principales	Le service de gestion de parc DOIT fournir, par établissement ou école, un dispositif permettant la gestion de l'inventaire des matériels (postes de travail, serveurs, écrans, vidéo projecteurs, TNI, VNI, appareils photos, équipements réseau et de sécurité, casques audio, caméras, imprimantes, microscopes…).	E	E
MCO-PAR-2	Fonctionnalités principales	L'outil de gestion de parc DEVRAIT permettre la catégorisation de ces matériels (fournisseurs, caractéristiques, vétusté, localisation, utilisation…).	R	R
MCO-PAR-3	Fonctionnalités principales	L'outil de gestion de parc DOIT permettre la recherche et les statistiques.	E	E
MCO-PAR-4	Fonctionnalités principales	L'outil de gestion de parc DEVRAIT permettre l'interfaçage avec le service de supervision (en particulier la gestion des incidents).	R	R
MCO-PAR-5	Fonctionnalités secondaires	L'outil de gestion de parc DEVRAIT permettre la gestion de la valeur (TCO) et des critères de remplacement et de mise au rebut.	R	R
MCO-PAR-6	Fonctionnalités secondaires	L'outil de gestion de parc DEVRAIT permettre la réservation de matériel.	R	R
MCO-PAR-7	Fonctionnalités secondaires	L'outil de gestion de parc PEUT permettre le prêt de matériel.	F	F

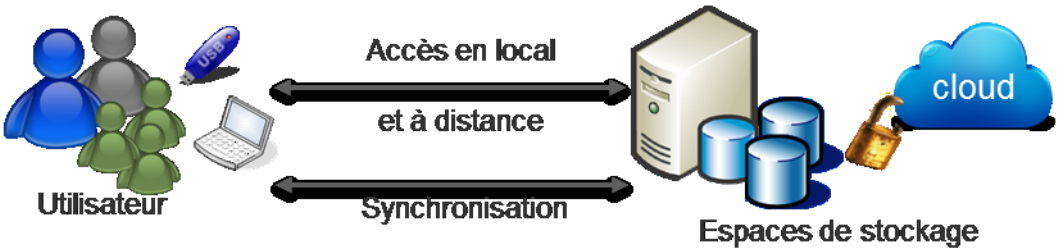
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
MCO-PAR-8	Découverte	Le service de gestion de parc DEVRAIT intégrer un mécanisme de découverte automatique des matériels connectés au réseau de l'établissement ou de l'école. Cela nécessite l'installation d'un agent sur les matériels de l'établissement ou de l'école, et cette recommandation devrait être prise en compte dans le choix des équipements.	R	R
MCO-PAR-9	Découverte	Les matériels hors parc (BYOD, visiteurs, prestataires…) connectés au réseau DEVRAIENT pouvoir être détectés afin de mesurer l'impact potentiel sur les infrastructures et leur sécurité	R	R
MCO-PAR-10	Consultation	Il existe des besoins de tableaux de bord concernant le matériel pour le ministère, les services académiques, les collectivités territoriales, les chefs d'établissement/directeurs d'école. Le service DOIT fournir aux chefs d'établissement/directeurs d'école le(s) tableau(x) de bord dont ils ont besoin, en particulier les éléments nécessaires au pilotage de l'établissement/école et au renseignement des enquêtes.	E	E
MCO-PAR-11	Mise au rebut	La mise au rebut des matériels DOIT respecter la réglementation, en termes environnemental et d'éventuelle cession de propriété (recyclage interne, dons (écoles, associations…), vente des domaines, sociétés privées de recyclage…) ;	E	E
MCO-PAR-12	BYOD	Une attention particulière doit être portée aux équipements hors parc (BYOD, visiteurs, prestataires…). On PEUT notamment leur appliquer des conditions spécifiques de raccordement au réseau de l'établissement ou de l'école.	F	F
MCO-PAR-13	Fonctionnalités secondaires	L'outil de gestion de parc PEUT intégrer la fonction de gestion du parc applicatif.	F	F

3.4 Services aux utilisateurs

3.4.1 Service de stockage

Service de stockage / synchronisation

Dans le cadre de leurs activités pédagogiques et administratives, les utilisateurs ont besoin d'espaces de stockage adaptés aux usages. Dans un objectif double de sécurité (sauvegarde des données) et de simplification des usages en situation de mobilité, le service de stockage DEVRAIT prévoir un mécanisme de synchronisation des données.



Le service DOIT offrir des espaces de stockage personnels et partagés à tout élève ou personnel travaillant dans l'établissement ou l'école.

Spécificité 1er degré

Le choix d'offrir un espace individuel à chaque élève du 1er degré est de la responsabilité des équipes pédagogiques.

Les espaces de stockage des Services d'Infrastructures viennent compléter si besoin les espaces de stockage fournis par les ENT. À ce titre les mécanismes permettant un accès transparent quel que soit l'endroit où est stockée la donnée sont à privilégier.

Impacts sur les infrastructures

Espaces partagés : Le service DOIT permettre de restreindre l'accès par utilisateur ou par groupe d'utilisateurs (notion d'espace de stockage partagé).

Postes partagés : Dans le cas où le poste est partagé entre plusieurs utilisateurs, les données personnelles ne DOIVENT être accessibles que par leurs propriétaires.

Multiplicité de supports : L'utilisation de plus en plus nomade des TIC favorise également la mise à disposition d'espaces de stockage sur des postes nomades, sur des supports amovibles (clés usb par exemple) ou sur des serveurs accessibles de partout (ex : ENT, services cloud).

Cloud : L'accès aux espaces cloud pose des questions de débit (bande passante d'accès à Internet), de confidentialité des données (localisation non maîtrisée), de réglementation (limiter les transferts de données à caractère personnel vers des pays assurant un niveau de protection suffisant).

Volumes : La capacité des espaces de stockage n'est pas illimitée. Des quotas DEVRAIENT donc être définis et il est légitime qu'ils soient surveillés en fonction des usages. Ces quotas DOIVENT tenir compte des élèves qui utilisent la LSF notamment ou beaucoup la vidéo. Ces usages nécessitent des espaces de stockage importants. Pour les élèves sourds pratiquant la LSF, la vidéo remplace l'écrit (LSF = langue première).

Stockage / Items	Dans l'ENT	Serveurs d'établissement/école	Support amovible (USB)	Cloud
Quotas	limité	limité (>ENT)	limité	illimité
Accès depuis l'extérieur	Oui	Oui	Pas toujours	Oui

Localisation des données	Établissement/école ou académie	Établissement/école	Non maîtrisé	Cloud public non maîtrisé
Contenus	Données établissement/école + données élèves	Données établissement/école + données classes	Non maîtrisé	Non maîtrisé

Synchronisation : Lorsque des applications ou des services enregistrent des données sur les terminaux de l'utilisateur, des mécanismes de synchronisation DEVRAIENT être proposés lorsque les débits réseau le permettent, afin de faciliter le nomadisme et d'augmenter le niveau de sécurité de ces données.

*Pour le stockage relatif aux données des terminaux mobiles, se référer au **dossier CARMO**.*

Impacts sur l'organisation

L'utilisateur doit être informé :

- sur les quotas de stockage des espaces qu'il utilise ;
- sur les procédures de sauvegarde/restauration mises en œuvre ;
- sur l'impact de ses choix lorsqu'il décide quelles données il stocke, où (dans l'ENT, sur les serveurs de l'établissement, dans le cloud…) et pourquoi.

Ces informations DOIVENT se retrouver dans les chartes d'établissement/écoles et/ou dans les conditions générales d'utilisation des services.

Les administrateurs techniques des espaces de stockage gèrent la capacité des espaces mais ne DOIVENT pas accéder au contenu de l'espace personnel (clairement identifié comme tel) sans l'accord de l'utilisateur ou d'une autorité judiciaire.

Les données privées de l'utilisateur DOIVENT être identifiées par les mots "PERSONNEL" ou "PRIVÉ" (nom de répertoire ou de fichier, en-tête de message…). Quand un répertoire est ainsi marqué, toute l'arborescence sous-jacente DOIT être considérée comme privée et accessible au(x) seul(s) propriétaire(s) des répertoires concernés. Ces mentions DOIVENT figurer dans la charte d'établissement / d'école.

Impacts sur la sécurité des SI

La confidentialité des données (et notamment leur caractère individuel, personnel ou privé) et la localisation des données (flux transfrontières) sont deux critères essentiels pour déterminer le lieu de stockage des données.

Les données sous la responsabilité de l'institution (espaces ENT, serveurs d'établissement/école en particulier) DOIVENT être sauvegardées régulièrement.

Si des données administratives sont stockées sur le poste de travail des personnels non enseignants (personnels de direction, personnels administratifs…) ou du directeur d'école, ces données doivent être protégées. Elles PEUVENT être chiffrées (chiffrement de masse) (voir **service Poste de travail** et **service de sauvegarde)**.

Aspects juridiques

Protection des mineurs : Les contenus stockés dans des espaces de stockage partagé et accessibles par un élève mineur DOIVENT respecter les exigences de protection des mineurs.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/protection-des-mineurs.html

Certaines données (journaux réglementaires par exemple) PEUVENT nécessiter la mise en place d'un mécanisme de contrôle d'intégrité (pour s'assurer qu'elles n'ont pas été modifiées).

Consulter régulièrement la rubrique « Protéger les données personnelles et la vie privée » sur http://eduscol.education.fr/internet-responsable/ressources/legamedia.html

Les fichiers structurés de données à caractère personnel DOIVENT être stockés dans des espaces qui respectent la réglementation.

Interaction avec d'autres services

☒ annuaire	☒ sauvegarde	☐ stockage / synchronisation
☒ poste de travail	☒ régénération de configurations	☒ messagerie électronique
☐ authentification	☒ supervision et exploitation	☒ communication temps réel
☒ sécurité et accès réseau	☒ gestion des journaux	☒ publication
☒ diffusion d'information	☐ gestion de parc	☒ recherche documentaire

UTI-ESF Service de stockage

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UTI-ESF-1	Stockage personnel	Le service DOIT offrir un espace de stockage individuel et sauvegardé à tout élève ou personnel travaillant dans l'établissement ou l'école. *Le choix d'offrir un espace individuel à chaque élève du 1er degré est de la responsabilité des équipes pédagogiques.	R*	E
UTI-ESF-2	Stockage partagé	Le service DOIT permettre de restreindre l'accès par utilisateur ou par groupe d'utilisateurs (notion d'espace de stockage partagé).	E	E
UTI-ESF-3	Poste partagé	Dans le cas où le poste est partagé entre plusieurs utilisateurs, les données personnelles ne DOIVENT être accessibles que par leurs propriétaires.	E	E
UTI-ESF-4	Gestion de quota	La capacité des espaces de stockage n'est pas illimitée. Des quotas DEVRAIENT donc être définis et il est légitime qu'ils soient surveillés en fonction des usages. Ces quotas DOIVENT tenir compte des élèves qui utilisent la LSF notamment ou beaucoup la vidéo.	R	R
UTI-ESF-5	Synchronisation	Dans un objectif double de sécurité (sauvegarde des données) et de simplification des usages en situation de mobilité, le service de stockage DEVRAIT prévoir un mécanisme de synchronisation des données. Synchronisation : Lorsque des applications ou des services enregistrent des données sur les terminaux de l'utilisateur, des mécanismes de synchronisation DEVRAIENT être proposés lorsque les débits réseau le permettent, afin de faciliter le nomadisme et d'augmenter le niveau de sécurité de ces données.	R	R

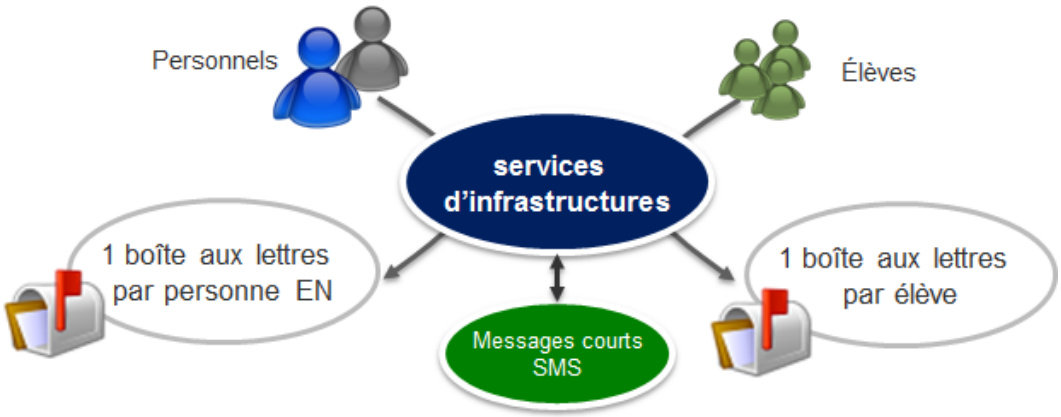
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UTI-ESF-6	Données personnelles/privées	Les données privées de l'utilisateur DOIVENT être identifiées par les mots "PERSONNEL" ou "PRIVÉ" (nom de répertoire ou de fichier, en-tête de message…). Quand un répertoire est ainsi marqué, toute l'arborescence sous-jacente DOIT être considérée comme privée et accessible au(x) seul(s) propriétaire(s) des répertoires concernés. Ces mentions DOIVENT figurer dans la charte d'établissement / d'école.	E	E
UTI-ESF-7	Formation/sensibilisation	L'utilisateur doit être informé : • sur les quotas de stockage des espaces qu'il utilise ; • sur les procédures de sauvegarde/restauration mises en œuvre ; • sur l'impact de ses choix lorsqu'il décide quelles données il stocke, où (dans l'ENT, sur les serveurs de l'établissement, dans le cloud…) et pourquoi. Ces informations DOIVENT se retrouver dans les chartes d'établissement/écoles et/ou dans les conditions générales d'utilisation des services.	R	R
UTI-ESF-8	Charte administrateur technique	Les administrateurs techniques des espaces de stockage gèrent la capacité des espaces mais ne DOIVENT pas accéder au contenu de l'espace personnel (clairement identifié comme tel) sans l'accord de l'utilisateur ou d'une autorité judiciaire.	E	E
UTI-ESF-9	Sauvegarde	Les données sous la responsabilité de l'institution (espaces ENT, serveurs d'établissement/école en particulier) DOIVENT être sauvegardées régulièrement.	E	E
UTI-ESF-10	Intégrité	Certaines données (journaux réglementaires par exemple) PEUVENT nécessiter la mise en place d'un mécanisme de contrôle d'intégrité (pour s'assurer qu'elles n'ont pas été modifiées).	F	F
UTI-ESF-11	Protection des mineurs	Les contenus stockés dans des espaces de stockage partagé et accessibles par un élève mineur DOIVENT respecter les exigences de protection des mineurs.	E	E

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UTI-ESF-12	Données à caractère personnel	Les fichiers structurés de données à caractère personnel DOIVENT être stockés dans des espaces qui respectent la réglementation.	E	E
UTI-ESF-13	Chiffrement	Si des données administratives sont stockées sur le poste de travail des personnels non enseignants (personnels de direction, personnels administratifs…) ou du directeur d'école, ces données doivent être protégées. Elles PEUVENT être chiffrées (chiffrement de masse).	F	F

3.4.2 service de messagerie électronique

Service de messagerie électronique

Le service de messagerie électronique (courrier électronique et SMS) permet aux utilisateurs situés dans l'école, dans l'établissement, voire en dehors, d'envoyer et de recevoir des courriers électroniques et/ou des sms.



Le service de messagerie électronique est souvent impliqué dans d'autres processus comme la gestion des devoirs, la publication web, les forums… Il remplit alors des fonctions de transport, d'alerte ou de notification pour d'autres applications ou services. C'est un des outils majeurs de la continuité pédagogique.

*Pour les services de messagerie électronique disponibles sur les terminaux mobiles, se référer au **dossier CARMO**.*

Impacts sur les infrastructures

Le service fournit les moyens pour accéder :

- à un service de courrier électronique :
- accès à une boîte aux lettres par agent, fournie par l'académie ; lorsque l'ENT est présent les agents disposent de deux boîtes électroniques ; il convient dès lors de mettre en place des fonctionnalités permettant une gestion unifiée de ces deux boîtes ;
- accès à une boîte aux lettres par élève ; dès que l'ENT est présent c'est lui qui la fournit.
- à un service de messages courts (sms).

Le service de messagerie électronique DOIT être accessible :

- à partir d'un logiciel client de messagerie;
- à partir d'une interface webmail.

Le service DOIT permettre de rédiger, envoyer, recevoir, ranger, archiver les courriers électroniques.

Le service de messages courts DOIT être accessible :

- à partir d'un logiciel installé sur un poste situé dans la zone « administrative » lorsqu'il est utilisé par les services de notification des applications (vie scolaire);
- à partir d'applications installées sur les postes de travail et/ou les terminaux mobiles (voir **dossier CARMO**) pour le dialogue en ligne (chat en anglais).

Le service DOIT permettre de rédiger, envoyer, recevoir, ranger, archiver les messages courts.

Impacts sur l'organisation

Courrier électronique

Les utilisateurs DOIVENT être informés des conséquences d'un stockage local des correspondances sur l'espace disque du poste de travail et sur les risques liés à la confidentialité et à la sauvegarde de ces données.

L'utilisation du service de courrier électronique par les élèves DOIT être soumise à des règles précisées dans la charte

de l'établissement ou de l'école.

L'adresse de la boîte aux lettres « élèves » DOIT être distincte de celle que les élèves utilisent éventuellement à titre privé.

Les messages entre élèves sont privés.

Les messages privés DOIVENT être identifiés comme tel sur la messagerie professionnelle, par exemple en mettant « [PRIVÉ] » ou « [PERSONNEL] » en tête du sujet, voire « [MESSAGE PRIVÉ] ». Cette mention DOIT être portée dans la charte de l'établissement ou de l'école.

Dans la boîte aux lettres électronique de l'utilisateur, les messages placés dans des dossiers nommés « personnel » ou « privé » DOIVENT être considérés comme tels, quel que soit le libellé de leur objet. Cette mention DOIT être portée dans la charte de l'établissement ou de l'école.

Messages courts

Les droits d'accès au service de messages courts DOIVENT être attribués par le chef d'établissement/directeur d'école.

Impacts sur la sécurité des SI

Aucune copie ni redirection automatique d'une boîte de messagerie professionnelle vers une boîte de messagerie privée ne DOIT être autorisée. Cette interdiction DOIT être rappelée dans la charte.

En effet, Les agents ne peuvent maîtriser a priori la nature de ce qui arrive dans leur boîte professionnelle. La redirection automatique vers une boîte aux lettres privée peut poser de graves problèmes de confidentialité, par exemple portant atteinte au secret ou la discrétion professionnelle dont ils doivent faire preuve dans l'exercice de leurs fonctions. Cela peut notamment porter atteinte à la vie privée des élèves (le plus souvent mineurs) qui leurs sont confiés.

Les éventuelles adresses privées des élèves ou des agents ne DEVRAIENT pas être utilisées pour les activités pédagogiques ou administratives.

Les agents ne DOIVENT pas communiquer avec les élèves en utilisant les éventuelles boîtes aux lettres privées de ces derniers.

Le service de courrier électronique DOIT être couplé avec un système anti-virus et un système anti-spam.
L'accès au service de messages courts DOIT être strictement réservé au personnel depuis un poste situé en zone « administrative », ou depuis le poste du directeur d'école et PEUT être protégé par authentification forte.

Toute diffusion de courrier électronique et de messages courts DOIT être tracée, identifiée et horodatée. (voir **service de gestion des journaux**).

Aspects juridiques

Un message électronique est un courrier privé lorsqu'il est envoyé à une ou plusieurs personnes physiques ou morales déterminées. Il est donc couvert par les dispositions légales concernant les correspondances privées.

L'usage privé des moyens mis à disposition dans le cadre professionnel DOIT demeurer proportionné au regard de la finalité première de ces moyens et des besoins prioritaires de la communauté scolaire.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/correspondance-privee-et-monde-numerique.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/archives/forum.html

Interaction avec d'autres services

☒ annuaire	☒ sauvegarde	☒ stockage / synchronisation
☒ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☐ supervision et exploitation	☒ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☒ publication
☒ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

UTI-MSG Service de messagerie électronique

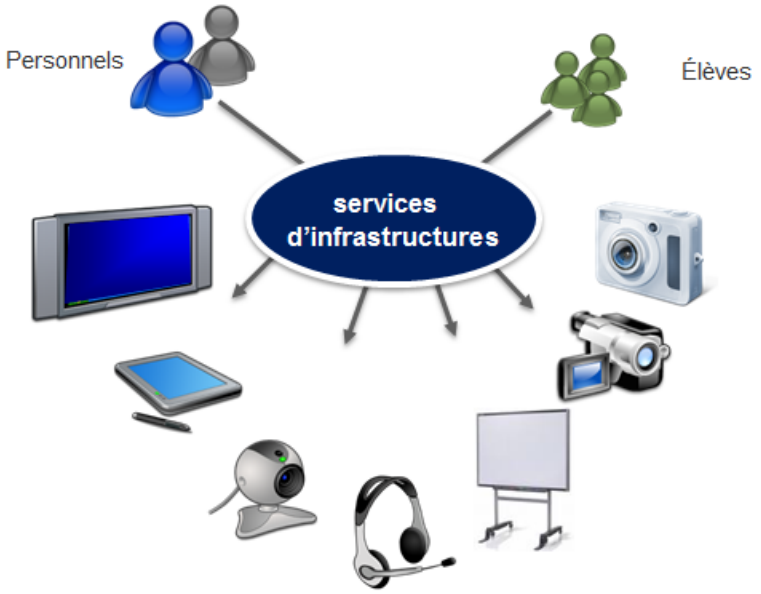
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UTI-MSG-1	Courrier électronique	Le service de messagerie électronique DOIT être accessible : • à partir d'un logiciel client de messagerie; • à partir de l'interface webmail. Le service DOIT permettre de rédiger, envoyer, recevoir, ranger, archiver les courriers électroniques.	E	E
UTI-MSG-2	Courrier électronique	L'utilisation du service de courrier électronique par les élèves DOIT être soumise à des règles précisées dans la charte de l'établissement ou de l'école.	E	E
UTI-MSG-3	Courrier électronique	L'adresse de la boîte aux lettres « élèves » DOIT être distincte de celle que les élèves utilisent éventuellement à titre privé.	E	E
UTI-MSG-4	Courrier électronique	Le service de courrier électronique DOIT être couplé avec un système anti-virus et un système anti-spam.	E	E
UTI-MSG-5	Courrier électronique	Les utilisateurs DOIVENT être informés des conséquences d'un stockage local des correspondances sur l'espace disque du poste de travail et sur les risques liés à la confidentialité et à la sauvegarde de ces données.	E	E
UTI-MSG-6	Courrier électronique	Dans la messagerie professionnelle, les messages privés DOIVENT être identifiés comme tel sur la messagerie professionnelle, par exemple en mettant « [PRIVÉ] » ou « [PERSONNEL] » en tête du sujet, voire « [MESSAGE PRIVÉ] ».	E	E
UTI-MSG-7	Courrier électronique	S'ils sont archivés sur le poste professionnel, les messages privés DOIVENT l'être dans des dossiers identifiés par leur nom ; par exemple « personnel » ou « privé ».	E	E

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UTI-MSG-8	Courrier électronique	Aucune copie ni redirection automatique d'une boîte de messagerie professionnelle vers une boîte de messagerie privée ne DOIT être autorisée. Cette interdiction DOIT être rappelée dans la charte.	E	E
UTI-MSG-9	Courrier électronique	Les éventuelles adresses privées des élèves ou des agents ne DEVRAIENT pas être utilisées pour les activités pédagogiques ou administratives.	R	R
UTI-MSG-10	Courrier électronique	Les agents ne DOIVENT pas communiquer avec les élèves en utilisant les éventuelles boîtes aux lettres privées de ces derniers.	E	E
UTI-MSG-11	Messages courts (sms)	Le service de messages courts DOIT être accessible : • à partir d'un logiciel installé sur un poste situé dans la zone « administrative » lorsqu'il est utilisé par les services de notification des applications (vie scolaire); • à partir d'applications installées sur les postes de travail et/ou les terminaux mobiles pour le dialogue en ligne (chat en anglais).	E	E
UTI-MSG-12	Messages courts (sms)	Les droits d'accès au service de messages courts DOIVENT être attribués par le chef d'établissement/directeur d'école.	E	E
UTI-MSG-13	Messages courts (sms)	L'accès au service de messages courts DOIT être strictement réservé au personnel depuis un poste situé en zone « administrative », ou depuis le poste du directeur d'école et PEUT être protégé par authentification forte.	E	E
UTI-MSG-14	Vie privée	L'usage privé des moyens mis à disposition dans le cadre professionnel DOIT demeurer proportionné au regard de la finalité première de ces moyens et des besoins prioritaires de la communauté scolaire.	E	E
UTI-MSG-15	Traçabilité	Toute diffusion de courrier électronique et de messages courts DOIT être tracée, identifiée et horodatée.	E	E

3.4.3 Service de communication temps réel

Service de communication temps réel

Le service de communication temps réel couvre les services qui permettent la mise en relation directe et instantanée entre plusieurs personnes.



Les Services d'Infrastructures fournissent les moyens d'accéder à des services rendus actuellement par des technologies de type dialogue en ligne (chat en anglais), téléphonie sur IP, web-conférence, visioconférence …

Ces services PEUVENT être fournis par l'ENT.

Ces services sont parfois « impliqués » dans d'autres services comme la publication web, les forums…

*Pour les services de communication temps réel disponibles sur les terminaux mobiles, se référer au **dossier CARMO**.*

Impacts sur les infrastructures

Les types de services de communication temps réel utilisables en établissement ou école sont fortement dépendants de la qualité et des débits réseau disponibles.

	<200 élèves	200 à 700 élèves	700 à 1000 élèves	> 1000 élèves
dialogue en ligne	Impact faible	Impact faible	Impact faible	Impact faible
Web-conférence	Impact faible	Impact faible	Impact moyen	Impact moyen
Visioconférence	Impact fort	Impact fort	Impact fort	Impact fort

Impacts sur l'organisation

Communication interpersonnelle

Certains de ces services sont utilisés dans le cadre de communication interpersonnelle (dialogue en ligne, téléphonie sur IP, web-conférence). L'accès à ces services est parfois associé à l'adresse de messagerie de l'utilisateur. Dans ces cas, seules les adresses fournies par l'institution DOIVENT être utilisées et les règles décrites dans le service de messagerie électronique dans les sections « impacts sur l'organisation », « impacts sur la sécurité des SI » et « aspects juridiques » DOIVENT s'appliquer.(voir **service de messagerie électronique**).

Impacts sur la sécurité des SI

Voir remarque sur la communication interpersonnelle.

Aspects juridiques

Voir remarque sur la communication interpersonnelle.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/correspondance-privee-et-monde-numerique.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/espace-dexpression-collective.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/archives/chat.html

Interaction avec d'autres services

☒ annuaire	☒ sauvegarde	☒ stockage / synchronisation
☒ poste de travail	☐ régénération de configurations	☒ messagerie électronique
☐ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☒ publication
☒ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

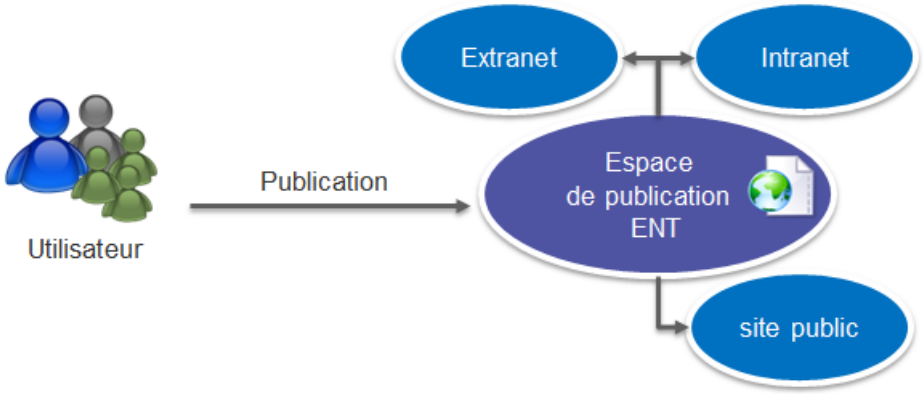
UTI-CTR Service de communication temps réel

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UTI-CTR-1	Fonctionnalités	Les services de communication temps réel PEUVENT être fournis par l'ENT	F	F
UTI-CTR-2	Accès	Certains de ces services sont utilisés dans le cadre de communication interpersonnelle (dialogue en ligne, téléphonie sur IP, web-conférence). L'accès à ces services est parfois associé à l'adresse de messagerie de l'utilisateur. Dans ces cas, seules les adresses fournies par l'institution DOIVENT être utilisées et les règles décrites dans le service de messagerie électronique dans les sections « impacts sur l'organisation », « impacts sur la sécurité des SI » et « aspects juridiques » DOIVENT s'appliquer.	E	E

3.4.4 service de publication

Service de publication

Les établissements et les écoles s'ouvrent vers l'extérieur et publient de plus en plus d'informations en ligne.



Le service offre les mécanismes et les procédures permettant de mettre à disposition des utilisateurs des outils de publication sur intranet et sur internet.

Ce service inclut les outils d'édition et de publication de contenus. Ces contenus peuvent être statiques ou dynamiques, intégrer des éléments multimédia (sons, images fixes, vidéo).

Ce service DEVRAIT être fourni par l'ENT.

Impacts sur les infrastructures

Les contenus PEUVENT être publiés en local via le service de diffusion d'information. (voir **service de diffusion**)

Les contenus PEUVENT être publiés sur internet, intranet, extranet.

Impacts sur l'organisation

Le chef d'établissement/le directeur d'école est la personne responsable des contenus édités et publiés par le personnel/les élèves de l'établissement/école. Des indications plus détaillées sont données sur le portail Internet responsable (http://eduscol.education.fr/internet-responsable/).

Les droits d'accès au service (en particulier la fonction de publication sur le site public) DOIVENT être attribués sous la responsabilité du chef d'établissement/directeur d'école.

Les règles d'usage du service DEVRAIENT être décrites dans ses conditions d'utilisation.

Le service de publication DEVRAIT permettre la mise en place d'un système de contrôle et de modération.

Impacts sur la sécurité des SI

L'accès à la fonctionnalité de publication DOIT être soumise à authentification et réservé aux personnes explicitement autorisées.

Les contenus ne sont pas toujours stockés sur des espaces pris en charge par le service de sauvegarde de l'établissement ou de l'école. Les conditions de sauvegarde et de restauration des contenus DOIVENT être précisées dans les CGU du service de publication.

Aspects juridiques

La responsabilité des auteurs, des modérateurs et de l'éditeur des contenus est engagée dans tous les cas prévus par la loi (injure, diffamation, atteinte à la vie privée, etc.). Consulter notamment les articles :

http://eduscol.education.fr/internet-responsable/ressources/legamedia/responsabilite-sur-le-web.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/publication-en-ligne-des-eleves.html

http://eduscol.education.fr/internet-responsable/ressources/legamedia/archives/blogue-ou-blog-information-prevention-sanction.html

Interaction avec d'autres services		
☐ annuaire	☒ sauvegarde	☐ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☐ publication
☒ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

UTI-PUB Service de publication

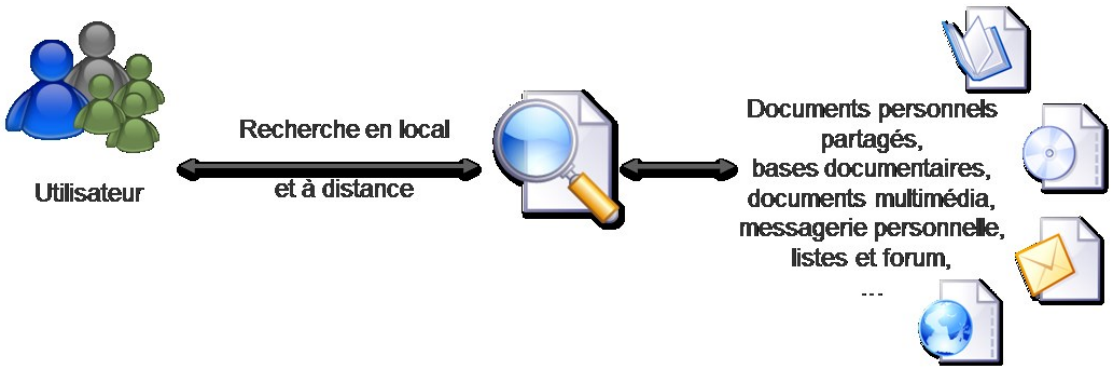
N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UTI-PUB-1	Fonctionnalités	Ce service DEVRAIT être fourni par l'ENT.	R	R
UTI-PUB-2	Modération	Le service de publication DEVRAIT permettre la mise en place d'un système de contrôle et de modération.	R	R
UTI-PUB-3	Publication	Les contenus PEUVENT être publiés en local via le service de diffusion d'information.	F	F
UTI-PUB-4	Publication	Les contenus PEUVENT être publiés sur internet.	F	F
UTI-PUB-5	Sauvegarde	Les contenus ne sont pas toujours stockés sur des espaces pris en charge par le service de sauvegarde de l'établissement ou de l'école. Les conditions de sauvegarde et de restauration des contenus DOIVENT être précisées dans les CGU du service de publication.	E	E
UTI-PUB-6	Accès	Les droits d'accès au service (en particulier la fonction de publication de site public) DOIVENT être attribués sous la responsabilité du chef d'établissement/directeur d'école.	E	E
UTI-PUB-7	Charte	Les règles d'usage du service DEVRAIENT être décrites dans la charte de l'établissement/école.	E	E
UTI-PUB-8	Authentification	L'accès à la fonctionnalité de publication DOIT être soumise à authentification et réservé aux personnes explicitement autorisées.	E	E

3.4.5 service de recherche documentaire

Service de recherche documentaire

Dans le but de faciliter l'accès des utilisateurs aux informations, ce service met à disposition un outil de recherche documentaire multi-critères s'appuyant sur des outils d'indexation.

La recherche peut porter sur des données structurées ou non (fichiers, fichiers audio/vidéo, pages Web, courriels et pièces attachées, forums, etc.).



Ce service DEVRAIT être accessible à partir de tout terminal connecté.

*Pour la recherche sur les données stockées sur les terminaux mobiles, se référer au **dossier CARMO**.*

Impacts sur les infrastructures

L'utilisateur DOIT pouvoir effectuer des recherches sur l'ensemble des données accessibles depuis le poste de travail professionnel (données stockées sur le poste, données de l'ENT, données stockées sur des serveurs académiques, bases documentaires, etc.).

Le service DEVRAIT permettre des recherches unifiées (notion de méta moteur) sur les données.

Impacts sur l'organisation

Les utilisateurs DOIVENT être informés sur l'intérêt et sur les impacts (confidentialité) du stockage des données sur des espaces partagés ouverts au service d'indexation et de recherche.

Impacts sur la sécurité des SI

Le service de sécurité DOIT veiller à ce que le service de recherche ne permette pas à l'utilisateur d'accéder à des données qu'il n'est pas autorisé à consulter.

Aspects juridiques

Protection des mineurs : Lorsqu'il existe, le filtrage des résultats affichés par le service de recherche DEVRAIT s'appuyer sur les mêmes règles que le dispositif de filtrage web.

http://eduscol.education.fr/internet-responsable/ressources/legamedia/protection-des-mineurs.html

http://educnum.fr/

Interaction avec d'autres services

☐ annuaire	☐ sauvegarde	☒ stockage / synchronisation
☐ poste de travail	☐ régénération de configurations	☐ messagerie électronique
☐ authentification	☐ supervision et exploitation	☐ communication temps réel
☒ sécurité et accès réseau	☐ gestion des journaux	☐ publication
☐ diffusion d'information	☐ gestion de parc	☐ recherche documentaire

UTI-REC Service de recherche documentaire

N°	Fonctions	Fonctionnalités / règles de gestion	Niveau de préconisation (scolaire)	
			1er D	2d D
UTI-REC-1	Recherche	L'utilisateur DOIT pouvoir effectuer des recherches sur l'ensemble des données accessibles depuis un poste de travail professionnel (données stockées sur le poste, données de l'ENT, données stockées sur des serveurs académiques, bases documentaires, etc.).	E	E
UTI-REC-2	Méta moteur	Le service DEVRAIT également permettre des recherches unifiées (notion de méta moteur) sur les données.	R	R
UTI-REC-3	Accès	Ce service DEVRAIT être accessible de partout.	R	R
UTI-REC-4	Données partagées	Les utilisateurs DOIVENT être informés sur l'intérêt et sur les impacts (confidentialité) du stockage des données sur des espaces partagés ouverts au service d'indexation et de recherche.	E	E
UTI-REC-5	Sécurité	Le service de sécurité DOIT veiller à ce que le service de recherche ne permette pas à l'utilisateur d'accéder à des données qu'il n'est pas autorisé à consulter.	E	E
UTI-REC-6	Protection des mineurs	L'accès des mineurs aux contenus remontés par le service de recherche DEVRAIT être contrôlé et protégé.	R	R

4. Historique S2i2e - CARINE

Le projet « Services internet-intranet d'établissements scolaires et d'écoles » (S2i2e) mené dans le cadre du « Schéma Directeur des Infrastructures », a été lancé en 2002, dans le but de donner le maximum de cohérence aux services internet et intranet mis en place pour des besoins spécifiques des équipes administratives et pédagogiques des établissements scolaires et des écoles primaires. Une note de cadrage a été réalisée, à destination des acteurs régionaux, notamment des académies en partenariat avec les collectivités territoriales, pour aider à la définition des infrastructures correspondantes.

Cette note de cadrage a été accompagnée de documents de référence thématiques destinés à accompagner la mise en place de ces services :

- un schéma de l'annuaire d'établissement, ancêtre de l'annuaire ENT ;
- des recommandations en termes de sécurité ;
- une charte type d'utilisation de l'internet, des réseaux et des services multimédias au sein de l'établissement scolaire et de l'école.

De 2002 à 2008, les usages des services numériques se sont considérablement développés grâce à l'effort accompli dans les académies, en partenariat avec les collectivités territoriales. L'ensemble des collèges et des lycées ont été raccordés à internet, et des solutions S2i2e ont été déployées dans la grande majorité des établissements du second degré.

Hormis ce développement des usages et des infrastructures numériques, d'autres facteurs ont conduit à revisiter le périmètre et la forme du référentiel des S2i2e, en particulier :

- la démarche de structuration des services TIC mis à la disposition des utilisateurs, engagée notamment à travers des projets tels que les espaces numériques de travail ;
- la nécessité de trouver des axes de rationalisation et d'amélioration des services S2i2e ;
- l'existence d'une forte tension sur les phases de maintenance, d'exploitation et de support aux utilisateurs, services fréquemment rendus à cette époque grâce à une multitude d'actions isolées, s'appuyant en partie sur de lourds investissements personnels ;
- le déficit constaté de cadre directeur sur le « maintien en condition opérationnelle » des S2i2e.

Le cadre de référence des S2i2e (CRS2i2e) 2008 introduisait donc plusieurs nouveautés :

- une vision davantage orientée vers les services eux-mêmes et leur description ;
- l'intégration des aspects de sécurité dans ces derniers, notamment sous forme de recommandations ;
- la prise en compte du service de bout en bout, ce qui incluait le poste de travail ;
- la prise en compte du nécessaire maintien en condition opérationnelle avec l'ajout de services y contribuant : configuration et régénération de station, sauvegarde, gestion des journaux, supervision et d'exploitation de l'infrastructure ;
- un apport sur le partage des responsabilités entre les différents acteurs locaux ;
- et l'abandon du schéma d'annuaire d'établissement, désormais traité dans le SDET.

Ce cadre de référence 2008 a été complété de deux fascicules :

- une annexe sur les indicateurs de pilotage et de suivi des S2i2e ;
- un complément sur le premier degré.

Depuis 2008, les besoins, les usages, les technologies et les offres de service ont évolué, plus encore qu'au cours des six années de la période précédente. Une étude a été lancée en 2014 afin d'identifier les points forts et les points faibles du référentiel de 2008.

Parmi les défauts relevés, se trouvaient l'absence de mises à jour régulières et un contenu trop « général » ne répondant pas suffisamment aux questions plus précises que se posaient les acteurs sur le terrain, par exemple en matière d'obligations et de réglementation. À l'inverse, l'intégration des indicateurs dans le référentiel S2i2e 2008 n'a pas semblé pertinente aux utilisateurs que nous avons interrogés et ils ont souhaité que les spécificités du premier degré soient traitées au sein du référentiel et non pas dans un fascicule complémentaire. C'est pourquoi le CARINE ne reprend pas en 2016 les deux compléments du CRS2i2e 2008.

Dans la même période, le plan numérique pour l'éducation a été outillé via l'élaboration d'un référentiel spécifique mis lui aussi au service des relations État-collectivités : ainsi le *Cadre de référence pour l'Accès aux Ressources pédagogiques via un équipement Mobile* (CARMO) encadre l'élaboration et la mise en œuvre des projets d'équipements mobiles pour l'accès aux ressources pédagogiques numériques.

La nouvelle version du CRS2i2e devait donc s'articuler avec ce nouvel élément. Un travail important a dû être effectué à cette fin. Ainsi, par exemple, le CARMO est-il cité dans 13 des 15 services du CARINE, de même que CARINE est cité à environ une douzaine d'endroits du CARMO v2.

Les évolutions sur le contenu et l'organisation du référentiel CARINE sont détaillées aux paragraphes 2.1 et 2.2 du chapitre 2.

5. Annexe

5.1 Glossaire

Terme	Définition
AVEC	Apportez Votre Équipement personnel de Communication En anglais : BYOD - Bring Your Own Device
BYOD	Bring Your Own Device En français : AVEC - Apportez Votre Équipement personnel de Communication
CARINE	CAdre de Référence des services d'Infrastructures Numériques d'Établissements scolaires et d'écoles
Charte d'établissement/école	Document définissant les droits et devoirs des utilisateurs des services numériques de l'établissement/école
Charte administrateur technique	Document définissant les droits et devoirs des administrateurs techniques des services numériques de l'établissement/école
Chiffrement de masse	Le « chiffrement de masse » désigne les solutions de chiffrement (cryptage) réalisé à la volée au niveau des partitions logiques des disques durs. Il peut aussi être mis en œuvre pour chiffrer des supports amovibles et permettre ainsi l'échange sécurisé d'informations.
Communauté éducative	Dans chaque école, collège ou lycée, la communauté éducative rassemble les élèves et tous ceux qui, dans l'établissement scolaire ou en relation avec lui, participent à l'accomplissement de ses missions. Elle réunit les personnels des écoles et établissements, les parents d'élèves, les collectivités territoriales, les associations éducatives complémentaires de l'enseignement public ainsi que les acteurs institutionnels, économiques et sociaux, associés au service public de l'éducation.
CRS2i2e	Cadre de Référence des S2i2e
Espace individuel	Espace dont l'usage est réservé à une personne. Des droits limités sur tout ou partie de cet espace peuvent être concédés à d'autres utilisateurs que le propriétaire, soit en vertu de règles organisationnelles écrites et connues de tous, soit par le propriétaire lui-même. Cet espace peut être visible d'un public plus ou moins étendu.
Espace personnel	Espace réservé à l'usage exclusif d'une personne et dont la confidentialité est garantie. Ne préjuge pas de l'usage principalement professionnel ou privé de l'espace.
Espace privé	Espace personnel réservé à des données considérées comme privées.
ENT (Espace Numérique de Travail)	Un espace numérique de travail (ENT) désigne un ensemble intégré de services numériques choisis et mis à disposition de tous les acteurs de la communauté éducative de l'école ou de l'établissement scolaire dans un cadre de confiance. Il constitue un point d'entrée unifié permettant à l'utilisateur d'accéder, selon son profil et son niveau d'habilitation, à ses services et contenus numériques. Il offre un lieu d'échange et de collaboration entre ses usagers, et avec les autres communautés en relation avec l'école ou l'établissement.
EPLE	Établissements Publics Locaux d'Enseignement
HTTP / HTTPS	Hyper Text Transport Protocol et sa version sécurisée basée sur SSL (Secure Socket Layer)
IA	Inspecteur d'académie
IEN	Inspecteur de l'éducation nationale

Terme	Définition
MAM	Mobile Application Management
MCM	Mobile Content Management
MDM	Mobile Device Management
MxM	Couvre les acronymes MDM, MAM et MCM
Mode dégradé	Fonctionnement des services de manière partielle ou ralentie suite à un dysfonctionnement. Une organisation particulière permet de poursuivre l'exploitation tout en préparant le dépannage.
PIA	Portail Intranet Académique
POP3 / IMAP4	Protocole standard pour la récupération de mèl sur un serveur SMTP
Poste partagé	Un poste de travail peut être partagé entre plusieurs utilisateurs (poste CDI par exemple). Les différents utilisateurs peuvent ou non, selon les choix de de l'EPLE/l'école, retrouver certains éléments personnalisés (forme et contenu du bureau, historique de navigation…). Leur usage peut également être identifié et tracé ou pas.
Proxy	On parle de serveur proxy pour désigner un dispositif qui gère des accès indirects à des ressources. Ce mécanisme dit « en coupure » permet la gestion de filtres (ex : listes d'exclusion d'url) et intègre parfois des mécanismes de cache pour optimiser les performances d'accès à des données fréquemment consultées.
PSSI	Guide d'élaboration de Politiques de Sécurité des Systèmes d'Information
PSSIE	Politique de Sécurité des Systèmes d'Information de l'État
RACINE et RACINE-AGRIATES	Réseau d'Accueil et de Consolidation des Intranets de l'Éducation Nationale Accès Généralisé aux Réseaux Internet Académiques et Territoriaux pour les Établissements Scolaires
Reverse-Proxy	Un proxy gère les sorties vers l'extérieur d'un SI. Un reverse-proxy gère les entrées vers le SI en intervenant en coupure entre les clients externes et les services internes.
RGI	Le Référentiel Général d'Interopérabilité (RGI) spécifie un ensemble des règles dont le respect s'impose à tous pour faciliter les échanges et rendre cohérent l'ensemble constitué des systèmes d'information du service public, pour assurer la simplicité d'intégration de nouveaux systèmes et pour faciliter l'évolution du système global ainsi que son utilisation par tous les acteurs. L'interconnexion des systèmes, favorisée par le RGI, ne doit pas se faire au détriment de la sécurité. (http://www.modernisation.gouv.fr)
RGS	Le Référentiel Général de Sécurité (RGS) apporte des méthodologies entre autres de conception, développement et exploitation permettant de renforcer la sécurité, et spécifie l'ensemble des règles que doivent respecter les fonctions de sécurité, comme l'identification, l'authentification, la signature... Par ailleurs, il définit des niveaux de sécurité sur lesquels doivent se caler les applications et les dispositifs afin d'assurer en la matière la cohérence des systèmes amenés à interagir. (http://www.modernisation.gouv.fr)
SDET	Schéma Directeur des Espaces Numériques de Travail
SDI	Schéma Directeur des Infrastructures
SDSSI	Schéma Directeur de la Sécurité des Systèmes d'Information
S2i2e	Services intranet/internet d'établissements scolaires et d'écoles
SI (Système d'Information)	Ensemble des ressources fonctionnelles, techniques et humaines qui permet de stocker, traiter, ou transmettre l'information
SMTP (Simple Mail Transfer Protocol)	Protocole standard pour les échanges de messages
SSO (Single Sign-On)	Mécanisme permettant à un utilisateur de s'authentifier une seule fois et d'obtenir

Terme	Définition
	l'accès à plusieurs ressources logicielles.
TIC	Technologies de l'information et de la communication
TICE	Technologies de l'information et de la communication pour l'éducation
USB (Universal Serial Bus)	Technologie permettant de brancher des périphériques sur un équipement
Visioconférence	Technologie qui permet de voir et de dialoguer avec un ou plusieurs (visioconférence multipoints) interlocuteurs.
XML (eXtensible Markup Language)	Langage informatique de balisage, dont l'objectif principal est de faciliter l'interopérabilité (échange automatisé de contenus entre systèmes d'informations hétérogènes).