Unité Développement pédagogique
Unité Informatique et Statistiques

Réf. : 2025-08-D-23-fr-1

Orig. : EN

CHARTE D'UTILISATION DES RESSOURCES INFORMATIQUES PAR LES MEMBRES DU PERSONNEL DES ÉCOLES EUROPEENNES ET DU BSG

Annexe au MEMO 2025-08-M-2

Sommaire

Schola Europaea

Bureau du Secrétaire général

Charte d'utilisation des ressources informatiques par les membres du personnel des Écoles européennes et du BSG

PRÉAMBULE

La présente Charte définit les règles de bon usage et de bon comportement quant à l'utilisation des ressources informatiques mises à disposition par les [techniciens informatiques/Unité Informatique] aux membres du personnel[1] et à tout invité[2] de l'[École européenne (ci-après dénommée « École ») / du Bureau du Secrétaire général (ci-après dénommé « BSG »)].

La mise en place de la présente Charte permet de protéger à la fois le BSG et les Écoles ainsi que les membres du personnel. L'utilisation inappropriée des ressources informatiques expose à des risques tels que les cyber-attaques, les violations de données, les problèmes de propriété intellectuelle, la compromission des systèmes et des services de réseau, ainsi que des problèmes juridiques.

La présente Charte annule et remplace tous les documents précédents à cet égard.

1. CHAMP D'APPLICATION

La présente Charte est fournie à la direction et aux membres du personnel [de l'École/du BSG] (ci-après dénommés « membres du personnel ») au cours du processus d'accueil ou ultérieurement lorsque la dernière version est disponible, ainsi qu'à tout invité bénéficiant des ressources informatiques [de l'École/du BSG].

Cette Charte constitue une annexe au Règlement intérieur de l'École et s'inscrit dans le cadre des lois et règlements en vigueur relatifs au droit d'auteur, aux droits de propriété intellectuelle, à la protection de la vie privée (incluant notamment le droit à l'image) et au traitement des données à caractère personnel, ainsi qu'à la criminalité informatique.

2. DÉFINITIONS

« Ressources informatiques » désigne généralement tous les dispositifs matériels (ordinateurs portables, postes de travail, téléphones mobiles, périphériques, tableaux blancs interactifs, etc.), les services de réseau, ainsi que toutes les ressources logicielles (applications, bases de données) accessibles localement ou à distance mis à disposition et administrés par l'EE (École européenne).

[1] Personnel administratif et de service (« PAS »), personnel détaché, personnel de direction recruté localement, membres du personnel temporaire (stagiaires, intérimaires).

[2] Toute personne qui est invitée au BSG/à l'École pour participer à une réunion, un groupe de travail ou une formation et qui bénéficie d'un accès aux ressources informatiques ou possède un compte des Écoles européennes.

« Unité Informatique » désigne l'Unité Informatique du BSG et les membres de son personnel.

« Département informatique » désigne le personnel informatique local des écoles.

« Services de mise en réseau » désigne la fourniture de services locaux et à distance tels que des applications, la messagerie, le web, les conférences, etc. par le biais de l'infrastructure de mise en réseau de l'EE.

« Utilisateur » désigne la personne ayant accès aux ressources informatiques et aux services de mise en réseau ou les utilisant, quel que soit son statut.

« DPD » Délégué(é) à la protection des données communément appelé DPO (Data protection Officer)

3. UTILISATION ACCEPTABLE ET PROPRIÉTE

Les ressources informatiques de [l'École/du BSG] sont destinées à être utilisées pour l'accomplissement des tâches professionnelles des membres du personnel, conformément à leur relation contractuelle ou statutaire avec [l'École/du BSG].

L'utilisation des ressources informatiques à des fins personnelles n'est pas interdite, mais les membres du personnel sont censés faire preuve de discernement et sont tenus de faire preuve de diligence et d'agir au mieux de leurs capacités pour éviter et/ou minimiser les risques lorsqu'ils utilisent les ressources à des fins personnelles, ainsi que pour rester productifs au travail lorsqu'ils les utilisent pour des questions d'ordre personnel.

Les membres du personnel doivent savoir que les dossiers et documents professionnels créés par le biais des ressources informatiques de l'[École/BSG] et entrant dans le cadre de leur emploi ou de leur détachement, ainsi que les tâches qui leur sont confiées, deviennent la propriété de l'[École/BSG].

À des fins de cybersécurité et de maintenance, les ressources informatiques [de l'École/du BSG], telles que les équipements, les systèmes et le trafic réseau, peuvent être surveillées à tout moment.

Tous les documents, licences, logiciels fournis par le biais des ressources informatiques sont la propriété [de l'École/du BSG] et ne doivent pas être copiés, altérés, modifiés ou transférés sans autorisation préalable.

4. RÈGLES GÉNÉRALES DE BONNE CONDUITE

4.1 Devoir de diligence

Les membres du personnel doivent faire preuve de prudence dans l'utilisation des ressources informatiques [de l'École/du BSG]. La perte, les dommages ou le vol des biens [de l'École/du BSG] doivent être signalés immédiatement [aux techniciens informatiques de l'École/à l'Unité Informatique].

Les membres du personnel sont tenus d'éteindre ou de mettre en veille les appareils lorsqu'ils ne les utilisent pas, de débrancher les chargeurs et de signaler les dysfonctionnements des équipements énergivores,

La négligence dans l'entretien et l'utilisation des biens du BSG peut être considérée comme un motif de sanction disciplinaire.

4.2 Devoir de confidentialité

Tous les membres du personnel sont tenus par une obligation légale de confidentialité[3] de protéger les informations à caractère personnel et non publiques auxquelles ils ont accès dans le cadre ou à l'occasion de l'exercice de leurs fonctions. Il leur est demandé de signer l'accord de confidentialité (annexe II) au cours du processus d'intégration ou ultérieurement lorsqu'une version actualisée de l'accord de confidentialité est disponible.

Plus particulièrement, ce devoir de confidentialité s'applique à toutes les informations mises à disposition par le biais des ressources informatiques fournies aux membres du personnel.

Dans le cas où les membres du personnel ont accès à des ressources qu'il serait inapproprié pour eux d'avoir, ils ont la responsabilité d'en informer l'Unité Informatique/les techniciens informatiques afin que le problème puisse être corrigé, ainsi que le DPD afin qu'une éventuelle violation des données puisse être évaluée.

5. RÈGLES SPÉCIFIQUES

5.1 Fichiers et documents

5.1.1 Stockage

Les membres du personnel doivent sauvegarder leurs fichiers et documents professionnels dans l'espace de stockage de leur appareil et/ou dans un espace de stockage partagé si d'autres collègues ont également besoin de les consulter.

Comme indiqué ci-dessus, les ressources informatiques sont destinées à être utilisées à des fins professionnelles, mais des documents privés peuvent être stockés sur l'appareil du membre du personnel **tant qu'ils ne contiennent pas de données à caractère personnel d'autres personnes.** Ces documents doivent être conservés dans un dossier appelé « PRIVÉ ».

Les membres du personnel doivent être conscients qu'en cas de violation de données, leurs documents privés peuvent être impactés.

5.1.2 Politique de bureau propre

Les membres du personnel doivent être conscients que laisser des documents sur leur bureau peut entraîner un accès non autorisé. Aucun document contenant des informations confidentielles ne doit être laissé sur les bureaux ou dans l'imprimante.

---

[3] Voir le Statut des membres du personnel des Écoles européennes :

- Article 18 du Statut du personnel détaché,
- Article 19 du Statut des membres du personnel d'encadrement des Écoles européennes recrutés localement

5.1.3 Interdiction

Les fichiers et/ou documents contraires à l'ordre public et aux bonnes mœurs ou illégaux, tels que les contenus racistes, xénophobes ou pornographiques, sont strictement interdits.

5.2 Utilisation du réseau et de l'internet

Les utilisateurs sont responsables de l'utilisation appropriée des ressources du réseau et de l'Internet.

L'utilisation d'un appareil numérique privé ne dispense pas les utilisateurs de suivre les règles énoncées dans la présente Charte, s'agissant du respect de leurs collègues et des membres de la communauté des Écoles européennes.

Par ailleurs, l'utilisation des médias sociaux, via les ressources informatiques ou un appareil numérique privé, ne dispense pas les utilisateurs d'être responsables du contenu qu'ils divulguent.

Les utilisateurs doivent :

- se connecter à leur compte professionnel uniquement à partir d'appareils sécurisés et éviter d'utiliser le Wi-Fi public gratuit,
- verrouiller leurs appareils lorsqu'ils les laissent sans surveillance,
- faire preuve d'une extrême prudence lorsqu'ils ouvrent des pièces jointes d'e-mails reçus d'expéditeurs inconnus,
- signaler [aux techniciens informatiques de l'École/à l'Unité Informatique] toute communication électronique suspecte,
- faire preuve de discernement quant au caractère raisonnable de l'utilisation personnelle.

Il est interdit aux utilisateurs :

- d'accéder à un serveur, à des données personnelles ou à un compte dans un but autre que l'exécution de leurs tâches professionnelles, même s'ils disposent d'un accès autorisé,
- d'envoyer des informations confidentielles à des destinataires non autorisés,
- de se connecter aux médias sociaux avec l'adresse e-mail liée à leur compte professionnel,
- de poster ou de publier des contenus sur les médias sociaux qui sont inappropriés ou nuisibles pour leurs collègues et les membres de la communauté des Écoles européennes,
- d'accéder, de télécharger ou de mettre en ligne du matériel obscène, offensant, discriminatoire ou autre interdit par la loi,
- de télécharger ou de charger illégalement tout matériel protégé par le droit d'auteur (c'est-à-dire images, musique, vidéo et logiciels),
- de télécharger, d'installer ou d'exécuter des mises à niveau, des mises à jour, des correctifs ou tout programme, logiciel quel qu'il soit,

- d'enquêter, de rechercher et de modifier la sécurité des solutions
- informatiques fournies sans autorisation préalable,
- d'utiliser toute faille de sécurité ou anomalie dans le fonctionnement du système.

5.3 Comptes et mots de passe

Les comptes sont créés (manuellement ou automatiquement) par le personnel de l'Unité Informatique. Ils sont temporaires, strictement personnels et ne peuvent être transférés. Ils doivent être désactivés dès lors que le titulaire quitte l'organisation.

L'utilisateur doit :

- définir son mot de passe conformément aux instructions fournies par l'Unité Informatique du BSG,
- utiliser un mot de passe fort et le garder confidentiel,
- informer immédiatement les administrateurs du système en cas de détection ou suspicion d'utilisation abusive du compte personnel.

Il est strictement interdit aux utilisateurs de partager et de révéler les identifiants et/ou le mot de passe de leur compte à des tiers (y compris les administrateurs du système) ou de permettre l'utilisation de leur compte par d'autres personnes.

5.4 Communications électroniques

5.4.1 Considérations générales

Les membres du personnel et les utilisateurs sont responsables de la gestion de leur courrier électronique, de leur chat et de tout autre contenu de communication lorsqu'ils utilisent les ressources informatiques [de l'École/du BSG].

Il leur est interdit :

- d'utiliser les listes d'adresses électroniques ou tout autre canal de communication à des fins autres que celles prévues par les objectifs professionnels,
- d'utiliser un langage inapproprié dans leurs communications,
- d'envoyer des communications non sollicitées (commerciales ou autres), non désirées ou harcelantes.

Puisque les communications électroniques sont destinées à l'accomplissement des tâches professionnelles des membres du personnel, l'utilisation de ces communications pour des questions d'ordre personnel doit être limitée. Dans ce cas, les membres du personnel doivent désigner leur communication électronique comme étant « PRIVÉE ».

Les boîtes aux lettres fonctionnelles et partagées ne doivent jamais être utilisées pour envoyer des communications électroniques qui ne sont pas liées aux tâches professionnelles du membre du personnel.

5.4.2 Absence d'un membre du personnel

Dans le cas où des membres du personnel ne pourraient pas accéder à leurs communications électroniques, ils sont tenus de prendre les dispositions nécessaires pour assurer la continuité des activités de l'École/du BSG :

- en activant une réponse automatique « out of office » dans des outils de communication tels qu'Outlook et en indiquant les coordonnées d'une autre personne/d'un collègue ainsi qu'un message d'état dans Teams par lequel les collègues sont informés de l'absence,
- en utilisant des dossiers partagés où l'information est accessible aux collègues suppléants et/ou à toute personne ayant un intérêt fonctionnel à y accéder pendant leur absence.

Il est déconseillé de transférer des e-mails pendant l'absence du membre du personnel, car le nouveau destinataire pourrait prendre connaissance d'informations potentiellement sensibles à l'insu de l'expéditeur ou du membre du personnel absent.

Dans des circonstances exceptionnelles et si aucun arrangement n'a pu être trouvé avant l'absence du membre du personnel, [l'École/le BSG] peut autoriser l'accès à la boîte aux lettres personnelle conformément aux conditions énoncées à ***l'annexe I***. Cet accès doit être conforme :

- au principe de finalité,
- au principe de proportionnalité,
- au principe de transparence.

En raison des exigences en matière de protection des données[4], l'accès aux boîtes aux lettres et aux documents des membres du personnel qui ont quitté le système des Écoles européennes (c'est-à-dire : licenciement ou départ) n'est pas possible. Tout le matériel et les documents liés au travail doivent être remis conformément aux instructions données par les supérieurs des membres du personnel avant leur départ (voir annexe III).

5.5 Enseignement

5.5.1 Enseignement et apprentissage à distance

Les enseignants doivent suivre les dispositions de la Politique d'enseignement et d'apprentissage à distance pour les Écoles européennes telle qu'approuvée par le Conseil supérieur le 29 mars 2021[5].

5.5.2 Ressources d'apprentissage numériques

Les enseignants qui doivent utiliser des ressources numériques conçues

[4] Principes de limitation de la finalité, de minimisation des données et de limitation du stockage.

[5] 2020-09-D-10.

et destinées à être utilisées à des fins éducatives et/ou pédagogiques doivent consulter le DPD de leur École.

Ce dernier évaluera ces ressources conformément à la Procédure d'utilisation d'une ressource d'apprentissage numériques au sein des Écoles européennes[6].

5.5.3 Médias sociaux

Une distinction est essentielle en ce qui concerne l'utilisation des médias sociaux :

- les médias sociaux ne sont pas couverts par la procédure susmentionnée, car les enseignants ne doivent pas utiliser les données personnelles des élèves sur les plateformes de médias sociaux,
- les enseignants ne doivent pas encourager les élèves à créer des comptes individuels sur les médias sociaux,
- les enseignants sont autorisés à créer un compte sur les médias sociaux à des fins éducatives et/ou pédagogiques conformément aux conditions énoncées à l'annexe IV.

Comme expliqué au paragraphe 5.2, les enseignants ne doivent pas créer un compte sur les médias sociaux avec leur adresse e-mail professionnelle pour des raisons de sécurité.

6. VIOLATION DES DONNÉES À CARACTÈRE PERSONNEL

Conformément au RGPD[7], une violation de données à caractère personnel est une violation de la sécurité entraînant la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

Conformément à la politique des Écoles européennes en matière de violation des données[8], les membres du personnel sont encouragés à agir rapidement et à signaler les violations de données au Secrétaire général/Directeur et/ou DPD Ils doivent également contacter [le département informatique local/l'Unité Informatique] afin de prendre immédiatement les mesures nécessaires pour prévenir et/ou atténuer toute conséquence négative.

[6] 2020-01-D-9 Annexe au MEMO 2019-12-M-3/GM. Cette procédure s'appuie sur les « intérêts légitimes poursuivis par le responsable du traitement » comme base juridique.

[7] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[8] 2020-05-D-7 Annexe au MEMO 2020-05-M-3-en-1/GM.

7. SUIVI

Pour des raisons de cybersécurité ainsi que pour sécuriser les opérations et la maintenance informatiques, les ressources informatiques et le trafic réseau peuvent être surveillés, analysés et testés pour vérifier qu'ils sont conformes aux lois applicables et dans les limites de celles-ci, de façon permanente ou ponctuelle, pour :

- la prévention des incidents et des attaques de cybersécurité,
- la prévention d'actes illicites ou diffamatoires, d'actes contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui,
- la protection des intérêts économiques ou financiers des écoles marquées comme confidentielles et la lutte contre les pratiques contraires,
- la sécurité et/ou le bon fonctionnement technique des systèmes informatiques du réseau des écoles, y compris la maîtrise des coûts y afférents, ainsi que la protection physique des installations scolaires,
- le respect de bonne foi des principes et règles d'utilisation des technologies de réseau établis dans le système des Écoles européennes.

Ce contrôle est principalement effectué par l'Unité informatique du BSG, spécifiquement pour le réseau administratif, tandis que les informaticiens de l'école sont responsables du réseau pédagogique.

La surveillance doit être effectuée par des moyens automatiques chaque fois que cela est possible. Toute intervention manuelle doit respecter le principe de proportionnalité, et l'administrateur du système doit informer le membre du personnel dont les informations sont surveillées des détails de l'intervention.

Si l'intervention manuelle a pour but d'assurer le respect de bonne foi des principes et règles d'utilisation des technologies de réseau établis dans le système des Écoles européennes, l'intervention doit être précédée d'une phase d'information préalable.

8. SANCTIONS

Toute violation des dispositions de la présente Charte peut faire l'objet de mesures disciplinaires conformément aux Statuts pertinents :

- titre VI du Statut du personnel détaché,
- chapitre VIII du Statut du personnel administratif et de service,
- chapitre VIII du Statut des chargés de cours.

9. DROIT NATIONAL

Les dispositions de la présente Charte ne portent pas atteinte à l'application de dispositions plus restrictives du droit national du pays d'accueil où se trouve [l'École/le BSG].

10. MODIFICATIONS

La présente Charte sera réexaminée au plus tard au cours de l'année scolaire 2027/28.

ANNEXE I

Schola Europaea

Bureau du Secrétaire général

Réf. : 2021-10-D-71-fr-1

Orig. : EN

Protocole sur l'accès aux e-mails et documents des membres du personnel en cas d'absence

Annexe à la Charte d'utilisation des ressources informatiques par les membres du personnel des Écoles européennes et du BSG (2025-08-D-23)

Protocole sur l'accès aux e-mails et documents des membres du personnel en cas d'absence

Sommaire

Protocole sur l'accès aux e-mails et documents des membres du personnel en cas d'absence

L'objectif des mesures préventives telles que celles indiquées au paragraphe 4.4.2 est de réduire la nécessité d'accéder à la boîte aux lettres et aux documents des membres du personnel en cas d'absence.

Lorsque ces mesures préventives ne contournent pas le besoin de l'employeur d'accéder aux courriels et/ou aux documents d'un employé absent ou lorsque de telles mesures n'ont pas été prises par l'employé avant l'absence, le présent protocole détermine comment cet accès doit être effectué pour se conformer aux considérations légales et de protection des données.

1. PRINCIPES DE FINALITE ET DE PROPORTIONNALITE

L'objectif d'assurer la continuité du service au sein [du BSG/de l'École] constitue un but légitime pour accéder à la boîte aux lettres et aux documents des membres du personnel pour autant i) qu'il y ait un sentiment d'urgence et ii) qu'il n'y ait pas d'autre moyen moins intrusif d'accéder aux informations nécessaires.

2. APPROBATION DU RESPONSABLE

Le besoin d'accès doit être dûment justifié par écrit à l'aide du formulaire ci-dessous.

Ce formulaire doit être envoyé au Secrétaire général/Directeur qui décidera d'autoriser ou non cet accès en fonction des circonstances et après avoir déterminé si :

- l'information nécessaire peut être accessible d'une manière moins intrusive,
- cet accès est nécessaire pour la continuité du service,
- cet accès est urgent ou peut être retardé compte tenu de la durée de l'absence de l'employé,
- cet accès devrait être autorisé dans le cadre de mesures de précaution supplémentaires par rapport à celles énoncées dans la présente annexe.

Le Secrétaire général/Directeur demandera également conseil au Délégué à la protection des données.

3. DROIT À L'INFORMATION

Les membres du personnel reçoivent la Charte informatique au cours du processus d'intégration ou ultérieurement lorsqu'une version actualisée est disponible. Par conséquent, ils sont informés de la possibilité d'accéder à leur boîte aux lettres et/ou à leurs documents dans les conditions prévues par le présent protocole.

Dans le cas où [le BSP/l'École] a besoin d'accéder à la boîte aux lettres et/ou aux documents d'un membre du personnel, celui-ci doit être contacté par téléphone et recevoir « *une explication détaillée de cet accès, soulignant la nécessité, l'urgence, la nature et la portée des informations recherchées*[9] ».

[9] Lignes directrices sur les données personnelles et les communications électroniques dans les institutions de l'UE, Conseil européen de la protection des données, février 2020.

Outre les informations à fournir en vertu de l'article 13 du RGPD[10], les membres du personnel doivent également être informés de leur droit d'opposition en vertu de l'article 21 du RGPD.

Lorsque le membre du personnel ne peut être joint et que la situation en question nécessite un accès urgent, le Secrétaire général/Directeur peut autoriser l'accès conformément au présent protocole.

4. ACCES LIMITE

4.1 Champ d'application limité

Lorsque l'autorisation a été donnée pour assurer la continuité du service, l'accès doit être limité aux courriels et/ou documents relatifs à la période d'absence du membre du personnel, ou à une période raisonnable précédant cette absence.

Le Secrétaire général/Directeur peut autoriser un accès plus étendu si les raisons ont été clairement expliquées dans la demande qui lui a été soumise et sont suffisamment justifiées.

En outre, seuls les courriels et/ou les documents relatifs à la demande initialement soumise pour approbation doivent être consultés.

Il ne peut être accédé aux courriels et documents portant la mention « PRIVE » comme indiqué dans la présente Charte.

4.2 Durée limitée

Une fois l'approbation accordée, l'accès aux informations des membres du personnel absents doit être limité à deux jours ouvrables.

4.3 Personnes autorisées limitées

Le Secrétaire général/Directeur désigne les personnes qui ont un intérêt légitime à accéder à la boîte aux lettres et/ou aux documents du membre du personnel.

Les techniciens informatiques des Écoles doivent demander les droits d'accès à l'Unité Informatique, car ils ne disposent pas de tels accès pour le réseau administratif.

L'accès aux informations nécessaires doit être effectué en présence d'un autre membre du personnel (par exemple, représentant du personnel, responsable hiérarchique, personne chargée des RH, Chef d'Unité) et si possible, sous la supervision du personnel informatique.

Le personnel informatique devra s'assurer que toutes les mesures nécessaires ont été prises, si besoin est, pour garantir la sécurité des

[10] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« Règlement général sur la protection des données »).

informations du membre du personnel (c'est-à-dire, changer les mots de passe).

5. PERIODES DE CONSERVATION

Il convient de consulter le DPD concernant le stockage des informations qui ont été récupérées lors de l'accès.

Schola Europaea

Bureau du Secrétaire général

Formulaire à utiliser pour demander l'accès aux e-mails et/ou documents d'un membre du personnel absent en cas d'urgence

Nom du membre du personnel absent *(dont les informations doivent être consultées)*	
Nom de la personne demandant l'accès	
Motifs de la demande d'accès *(Pourquoi y a-t-il un sentiment d'urgence, pourquoi est-ce le seul moyen d'accéder aux informations nécessaires, etc.)*	
Type d'informations requises	
Conclusion du Secrétaire général/Directeur	☐ Accès accordé ☐ Accès refusé Date et heure : Signature :
Le membre du personnel a été informé par téléphone	☐ Oui … date/heure …… ☐ La personne n'était pas joignable
Nom du ou des membres du personnel qui seront présents lors de l'accès	

A remplir **pendant** l'accès :

Date effective d'accès	Date et heure …
Nom des personnes présentes lors de l'accès	
Observations *(Type d'informations à consulter et délai d'exécution)*	

A remplir à **la fin** de l'accès :

Fin de l'accès	Date et heure …
Observations *[Type d'informations consultées et délai d'exécution, résultats de la consultation (les informations recherchées ont été trouvées ou non)]*	
Nom et signature de la personne ayant eu l'accès	

ANNEXE II

Schola Europaea

Bureau du Secrétaire général

Réf. : 2021-10-D-73-fr-1

Orig. : EN

Accord de confidentialité

Annexe à la Charte d'utilisation des ressources informatiques par les membres du personnel des Écoles européennes et du BSG (2025-08-D-23)

Schola Europaea

Bureau du Secrétaire général

Accord de confidentialité

Conformément au statut qui lui est applicable, tout membre du personnel est tenu d'observer la plus grande discrétion sur les faits et informations dont il a connaissance dans l'exercice ou à l'occasion de l'exercice de ses fonctions.

Je, soussigné(e), M./Mme _____, travaillant en tant que _____ [au BSG/à l'École européenne] (ci-après dénommé(e) « BSG/Ecole »), ayant accès à des informations confidentielles et des données personnelles appartenant [au BSG/à l'École européenne], déclare reconnaître la confidentialité desdites données.

Je m'engage donc, conformément aux exigences du statut qui m'est applicable et du RGPD[11], à prendre toutes les précautions nécessaires dans le cadre de mes fonctions pour protéger la confidentialité des informations auxquelles j'ai accès, et notamment pour empêcher qu'elles ne soient altérées, endommagées ou communiquées à des personnes non expressément autorisées à les recevoir.

Je m'engage :

- à ne pas utiliser les données auxquelles je pourrais avoir accès à d'autres fins que celles prévues dans le cadre de mes fonctions.
- à ne pas divulguer ces données à toute autre personne que celles dûment autorisées, en vertu de leurs fonctions, à recevoir ces données ;
- à ne faire aucune copie de ces données sauf si cela est nécessaire à l'exercice de mes fonctions ;
- à prendre toutes les précautions nécessaires pour préserver la sécurité physique de ces données ;

[11] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« Règlement général sur la protection des données »).

- à veiller, dans les limites de mon autorité, à ce que seuls des moyens de communication sécurisés soient utilisés pour transférer ces données et à consulter le DPD en cas de doute ;

- à garantir l'utilisation respectueuse des technologies de l'IA conformément aux réglementations et aux politiques des Écoles européennes.

- en cas de cessation de mes fonctions, à restituer toutes les données, documents et tout support d'information relatifs à ces données.

Cet accord de confidentialité, qui est en vigueur pour la durée de mon emploi, restera en vigueur sans limitation de durée après ma cessation d'emploi, quelle qu'en soit la cause, dans la mesure où cet accord concerne l'utilisation et la divulgation de données personnelles ou d'informations confidentielles.

J'ai été informé(e) que toute violation de cet engagement m'exposera à des actions et sanctions disciplinaires et pénales conformément aux dispositions légales en vigueur.

(Ville) _____ le _____ en__copies.

Nom :

Signature :

ANNEXE III

Schola Europaea

Bureau du Secrétaire général

Réf. : 2021-10-D-74-fr-1

Orig. : EN

Lignes directrices pour la procédure de départ des membres du personnel

Annexe à la Charte d'utilisation des ressources informatiques par les membres du personnel des Écoles européennes et du BSG (2025-08-D-23)

LIGNES DIRECTRICES POUR LA PROCÉDURE DE DÉPART DES MEMBRES DU PERSONNEL

Sommaire

LIGNES DIRECTRICES POUR LA PROCÉDURE DE DÉPART DES MEMBRES DU PERSONNEL

Le BSG et les Écoles européennes doivent prévoir une procédure qui définit la procédure à suivre lorsqu'un membre du personnel est transféré vers une autre [Unité/École] ou quitte définitivement [le BSG/l'École].

L'objectif d'une telle procédure est de garantir une perturbation minimale des activités de travail et le transfert efficace de tous les contenus d'information, dans le respect des exigences en matière de protection des données.

Cette procédure doit couvrir au moins les éléments suivants :

1. **RESPONSABILITÉ**

   La procédure de transfert doit être mise en œuvre principalement par le membre du personnel sortant. Le [responsable hiérarchique du membre du personnel sortant/la personne en charge des RH dans l'École] est chargé(e) d'initier et de suivre le processus de transfert et de s'assurer qu'il est réalisé dans le meilleur intérêt [du BSG/de l'École] pour la continuité de ses activités.

2. **PROCESSUS DE TRANSFERT DES TRAVAUX**

   - Définition d'un plan et d'un calendrier pour le transfert des informations du BSG/de l'École (dossiers, fichiers, documents, etc.),
   - Transfert des tâches et des connaissances au remplaçant du membre du personnel sortant (par exemple, activités quotidiennes, questions en cours, accès aux informations pertinentes, etc.),
   - Transfert d'informations sous forme électronique et papier (par exemple, liste de contrôle des dossiers, documents, archives, copie des courriels pertinents, etc.) à l'endroit désigné et [au responsable hiérarchique du membre du personnel sortant/à la personne chargée des RH dans l'École].

     Ces informations doivent être stockées sur un support de stockage d'informations partagé (par ex. serveurs, armoires de rangement, etc.) utilisé par l'Unité, le département et/ou les collègues.

3. **REMISE DE L'ÉQUIPEMENT**

   [Le responsable hiérarchique/la personne en charge des RH dans l'école] est chargé de :

   - compiler une liste de tous les équipements et articles à récupérer/transférer et prévoir qui est responsable de la récupération de(s) équipement(s) professionnel(s), des badges, des clés ainsi que des mobiles professionnels [du BSG/de l'École], le cas échéant.
   - planifier et d'informer le membre du personnel sortant des modalités de la remise à la (aux) personne(s) désignée(s) et du calendrier défini.

4. AUTORISATIONS ET ACCÈS

- Avant son départ, le membre du personnel en question doit être autorisé :
    i. à rassembler ses affaires personnelles,
    ii. à collecter ou supprimer ses communications électroniques privées,
    iii. à détruire les documents qui ne sont plus nécessaires pour assurer la continuité des activités du BSG/de l'École.
- Le membre du personnel doit être informé de la désactivation de son compte et de la révocation de tous ses droits d'accès aux ressources [du BSG/de l'École] le jour de la fin de son contrat. Le contenu du compte du membre du personnel sortant sera supprimé après l'expiration de la période de conservation de trente jours, sans préjudice des droits énoncés au chapitre III du RGPD.
- Le département informatique local ou l'Unité Informatique/les informaticiens du BSG et le ServiceDesk doivent être dûment informés par le [supérieur hiérarchique/responsable des RH du BSG/de l'École] par le biais d'une demande de service adressée à [OSG-ICT-SERVICEDESK@eursc.eu (pour le BSG)/ou à ES-ICT-SERVICEDESK@eursc. eu (pour les Écoles)] pour exiger la désactivation de tous les comptes appartenant au membre du personnel sortant et la suppression de tout le contenu de ces comptes après un mois civil.

ANNEXE IV

Schola Europaea

Bureau du Secrétaire général

Réf. : 2021-12-D-09-fr-1

Orig. : EN

Lignes directrices pour l'utilisation des médias sociaux par le personnel des EE

Annexe à la Charte d'utilisation des ressources informatiques par les membres du personnel des Écoles européennes et du BSG (2025-08-D-23)

LIGNES DIRECTRICES POUR L'UTILISATION DES MÉDIAS SOCIAUX PAR LES ENSEIGNANTS

Ces lignes directrices ont pour but d'aider les enseignants à utiliser les médias sociaux en classe avec leurs élèves d'une manière responsable, sûre et fiable, sans nuire à la réputation de l'école ou de sa communauté.

REMARQUES PRELIMINAIRES

Afin de garantir le respect des exigences du RGPD et des lois nationales applicables, les Écoles européennes n'autorisent pas les élèves à créer des comptes individuels sur les médias sociaux, à l'aide de leurs comptes/identifiants de l'école, comme le prévoit la Charte informatique pour les élèves.

Ces plateformes n'offrent aucune garantie en termes de respect de la vie privée, car leurs conditions d'utilisation ne peuvent être négociées par le Directeur de l'école.

Toutefois, l'École peut autoriser la création d'un compte au nom de la classe dans les conditions énoncées ci-dessous.

1. **DÉFINITION DES OBJECTIFS PÉDAGOGIQUES**

   L'enseignant doit guider les élèves vers une utilisation sécurisée et responsable. Les finalités pédagogiques recherchées par l'enseignant lors de la création d'un compte sur les médias sociaux pour la classe doivent être définies au préalable.

   Ces objectifs peuvent inclure :

   - l'acquisition de compétences numériques,
   - la sensibilisation à Internet (*aspects juridiques, droit à l'image, attitude responsable, e-réputation, conscience des dangers*),
   - l'éducation par les médias écrits et audiovisuels,
   - le développement de l'esprit critique.

2. **CRÉATION DE COMPTE**

   L'enseignant est responsable de créer le compte et le mot de passe ne doit pas être partagé avec les élèves.

   Le compte doit être créé avec une adresse e-mail « temporaire/disponible », utilisée pour une courte période, qui peut être supprimée dès lors qu'elle n'est plus utile.

   En d'autres termes, l'adresse e-mail « temporaire/disponible » est une adresse e-mail créée spécifiquement pour la création du compte sur les médias sociaux.

   Cette adresse e-mail est nécessaire pour éviter les menaces de sécurité qui pourraient compromettre les informations des enseignants ainsi que celles de l'École.

3. CHARTE DES MÉDIAS SOCIAUX

L'enseignant doit rédiger une Charte d'utilisation des médias sociaux avec les élèves afin de définir les objectifs du projet et de les sensibiliser à l'utilisation d'Internet.