UNIVERSITÉ BOURGOGNE EUROPE

# DÉLIBÉRATION
# du conseil d'administration
# de l'Université Bourgogne Europe

## Séance du 8 juillet 2025

---

Délibération n° 2025 – 08/07/2025 – 5

*Nouvelles versions des chartes du numérique à l'Université Bourgogne Europe*

---

- VU le code de l'éducation
- VU le décret n° 2024-1157 du 4 décembre 2024 portant création de l'Université Bourgogne Europe et approbation de ses statuts
- VU les statuts de l'Université Bourgogne Europe
- VU l'avis du comité social d'administration rendu en sa séance du 11 juin 2025

| | |
|---|---|
| Effectif statutaire : 38<br>Membres en exercice : 38<br>Quorum : 19<br><br>Membres présents : 25<br>Membres représentés : 8<br>Total : 33 | **Refus de vote : 0**<br>**Abstention(s) : 0**<br><br>**Suffrages exprimés : 33**<br><br>**Pour : 33**<br><br>**Contre : 0** |

Le conseil d'administration, après en avoir délibéré, **approuve les nouvelles versions des chartes du numérique à l'Université Bourgogne Europe.**

Dijon, le 9 juillet 2025

Le Président de l'Université Bourgogne Europe,

Vincent THOMAS

*P.J. : Charte du bon usage des moyens numériques UBE 2025 – Guide des bonnes pratiques charte numérique UBE 2025 – Charte d'utilisation de la messagerie électronique charte numérique UBE 2025 – Annexe juridique charte numérique UBE 2025 – Charte de déontologie charte numérique UBE 2025 – Charte syndicats charte numérique UBE 2025*

Délibération transmise à la rectrice de la région académique Bourgogne-Franche-Comté
Chancelière de l'Université Bourgogne Europe

Délibération publiée sur le site Internet de l'établissement

# CHARTE DE BON USAGE DES MOYENS NUMÉRIQUES DE L'UNIVERSITÉ BOURGOGNE EUROPE

*1 – Document principal*

## S'applique à :

Tout personnel, étudiant et usager du système d'information de l'Université Bourgogne Europe (UBE)
Ci-dessous désignés par l'« utilisateur »

## Par :

L'Université Bourgogne Europe
Ci-dessous désignée par « l'Université » ou « UBE »

**Ce document est la mise à jour de la charte d'usage des TIC votée en CA le 28/06/2007**

**Charte présentée au CSA du 11/06/2025**

**Charte mise à jour et votée par le conseil d'administration de l'Université Bourgogne Europe le 08/07/2025. Cette charte vaut pour règlement intérieur.**

ENT : Environnement Numérique de Travail

**https://ent.ube.fr**

## Préambule

La présente charte a pour objet de fixer les règles d'usage des moyens numériques de l'Université Bourgogne Europe.

Ces règles ont pour but de contribuer à la sécurité du système d'information et de garantir l'intégrité et la confidentialité des données qui y sont hébergées.

L'usage raisonné des moyens numériques concourt par ailleurs à une conciliation saine et équilibrée des temps de vie professionnel et personnel, ainsi qu'à une plus grande sobriété numérique.

# SOMMAIRE

# Introduction

Le *système d'information* est constitué de l'ensemble des moyens matériels, logiciels, applications, bases de données et réseaux de télécommunications, pouvant être mis à la disposition de l'*utilisateur*.

L'informatique nomade, constituée par les assistants personnels, les ordinateurs portables, les téléphones portables …, est également un des éléments constitutifs du système d'information.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent et notamment, la sécurité, la performance des traitements et la conservation des données personnelles.

La présente charte définit les règles d'usage et de sécurité que l'institution et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

**La charte est accompagnée de plusieurs annexes dont une annexe juridique qui rappelle les dispositions législatives en vigueur pour son application, d'une charte de messagerie et d'un guide d'utilisation définissant les principales pratiques d'usage notamment. La liste des annexes est précisée dans l'article « Annexes et entrée en vigueur de la charte ».**

L'Université Bourgogne Europe porte à la connaissance de l'utilisateur la présente charte.

## Engagements de l'institution

L'Université Bourgogne Europe s'engage à mettre en œuvre les moyens nécessaires destinés à assurer la sécurité du système d'information et la protection des utilisateurs.
Elle facilite l'accès des utilisateurs aux ressources du système d'information qui sont dédiées à l'enseignement, à la recherche, à la documentation et à la gestion de l'Université.
Les ressources mises à disposition sont prioritairement à usage universitaire, mais l'institution est tenue de respecter la vie privée de chacun.

## Engagement de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect de l'ensemble des chartes et des règles d'éthique et de déontologie.

Les utilisateurs ont une responsabilité particulière dans l'utilisation qu'ils font des ressources mises à leur disposition par l'Université.
En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

## Article 1. Champ d'application

**Les règles d'usage des moyens numériques figurant dans la présente charte s'appliquent à l'Université de Bourgogne Europe et à l'ensemble de ses utilisateurs.**

**Par l'expression « moyens numériques », la présente charte vise tous les éléments ou toutes les ressources constituant le système d'information de l'université. Ainsi, les moyens numériques représentent l'ensemble des logiciels et matériels, outils informatiques et services numériques, que l'université met à disposition de ses utilisateurs.**

**Les « utilisateurs », au sens de la présente charte, sont définis comme l'ensemble des personnes ayant obtenu l'autorisation d'accéder au système d'information de l'université.**
Un utilisateur peut être une personne physique (étudiant, enseignant, chercheur, ingénieur, technicien, administratif, personnel de service, personnel temporaire, stagiaire, émérite ...) autorisée à accéder à l'une des ressources du système d'information.

**L'accès se réalise au moyen d'un compte nominatif créé dans le système d'information au profit de l'utilisateur, pour la durée de son activité à l'université. Appelé « compte informatique », il est formé d'un identifiant - ou « login » - propre à un utilisateur et attribué lors de son arrivée à l'université, et d'un mot de passe choisi par l'utilisateur. Le cycle de vie des comptes est régi par un ensemble de règles qui garantissent l'expiration du compte au départ de l'utilisateur, l'université ne reconnaît pas un droit général au maintien d'un accès au système d'information et, par voie de conséquence au maintien du compte, après le départ de l'utilisateur.**

**Les dispositions de la présente charte s'appliquent également aux utilisateurs membres du personnel de l'université autorisés à exercer leurs missions dans les conditions de télétravail.**

**Les utilisateurs ayant des fonctions d'administrateur des moyens numériques seront soumis à une charte complémentaire et spécifique précisant leurs obligations particulières.**

**Les usages relevant de l'activité des organisations syndicales sont régis par un document spécifique qui complète la présente charte.**

**L'ensemble de ces documents est accessible en ligne et notamment sur l'environnement numérique de travail de l'université.**

**Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'université ainsi qu'à l'ensemble des utilisateurs.**

# Article 2. Conditions d'utilisation des systèmes d'information et moyens numériques

## *2.1 Utilisation universitaire professionnelle / privée*

**L'université met à la disposition de ses utilisateurs un ensemble d'outils et de services numériques à des fins professionnelles.**
**Au sens de la présente charte, l'usage des moyens numériques présente un caractère professionnel lorsqu'il intervient :**

- **dans le cadre des missions confiées par l'université, pour les utilisateurs membres de son personnel : enseignants-chercheurs, enseignants, personnels administratifs, techniques, sociaux et de santé, mais également ses prestataires et partenaires ;**
- **dans le cadre des activités pédagogiques, pour ses utilisateurs étudiants.**

Par opposition, l'utilisation à des fins privées doit être non **lucrative** et limitée, tant dans la fréquence que dans la durée. Elle ne doit nuire ni à la qualité du travail de l'utilisateur, ni au temps qu'il y consacre, ni au bon fonctionnement du service (vie privée résiduelle).

Cette utilisation à des fins privées doit se faire dans le strict respect des principes de sécurité exposés à l'article III de la présente charte. Son impact doit demeurer négligeable pour l'université : elle ne doit en conséquence entraîner aucun surcoût pour l'établissement, que celui-ci soit financier ou énergétique, ni aucune augmentation des risques pour la sécurité des données et des équipements professionnels.

Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace prévu à cet effet et identifié sans ambiguïté comme tel. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.

Ainsi, tout utilisateur manifestera le caractère extra-professionnel d'une partie de ses données en adoptant, exclusivement, le terme « privé », pour nommer le dossier de fichiers ou l'objet du message contenant ces informations.

## *2.2 Continuité de service : gestion des absences et des départs*

**Lors d'un départ définitif ou d'une absence ponctuelle, l'utilisateur informe sa hiérarchie des modalités d'accès aux applications et données permettant d'assurer la continuité de service.**

**Les mesures de conservation des données professionnelles sont définies avec le responsable hiérarchique désigné au sein de l'université.**

**Le responsable hiérarchique d'un utilisateur veillera – en cas de départ de ce dernier – à la suppression des accès ou – en cas de mobilité interne – à la réévaluation des accès et des droits dans les applications professionnelles.**

L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé.

L'utilisateur doit impérativement stocker les documents à caractère professionnel en utilisant les services de stockage, tels que : serveur de fichiers, Cloud, GED, dont les serveurs sont hébergés à l'UBE. Il est également rappelé que les utilisateurs ne doivent pas stocker les fichiers sur leur PC, sauf de manière temporaire.

# Article 3. Principes de sécurité

## *3.1 Règles de sécurité applicables*

L'université met en œuvre les mécanismes de protection appropriés sur les moyens numériques mis à la disposition des utilisateurs.

L'utilisateur est informé que les mots de passe constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas un caractère personnel aux outils informatiques protégés.

Les niveaux d'accès ouverts à l'utilisateur sont définis en considération de la mission qui lui est confiée. La sécurité des ressources mises à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des mots de passe ;
- de garder strictement confidentiel(s) son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers ;
- de respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre utilisateur, ni chercher à les connaître.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

- **de la part de l'université :**
  - veiller à ce que les ressources sensibles ne soient pas accessibles en cas d'absence (en dehors des mesures de continuité mises en place par la hiérarchie) ;
  - limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- **de la part de l'utilisateur :**
  - si l'utilisateur ne bénéficie pas d'une habilitation explicite, il doit s'interdire d'accéder ou tenter d'accéder à des ressources du système d'information, même si cet accès est techniquement possible ;
  - ne pas connecter directement aux réseaux locaux des matériels non confiés ou non autorisés par l'université. L'autorisation devra être demandée au préalable de l'achat de matériel ;
  - ne pas installer, télécharger ou utiliser sur le matériel de l'université, de logiciels ou progiciels sans y être autorisé ;
  - se conformer aux dispositifs mis en place par l'université pour lutter contre la cybermalveillance.

## 3.2 Devoir de signalement et d'information

L'université doit porter à la connaissance de l'utilisateur tout élément susceptible de lui permettre d'apprécier le niveau de risque encouru dans l'utilisation du système d'information.

L'utilisateur doit avertir dans les meilleurs délais, son supérieur hiérarchique, le chargé de sécurité du système d'information (CSSI), ou à défaut au RSSI de l'établissement de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, ou toute faille de sécurité. Il signale également à son chargé de sécurité du système d'information (CSSI), ou à défaut au RSSI de l'établissement, toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation ou à l'habilitation d'un utilisateur.

## 3.3 Mesures de contrôle de la sécurité

L'utilisateur est informé que :

- pour effectuer la maintenance corrective, curative ou évolutive, l'université se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- une maintenance à distance est précédée d'une information de l'utilisateur ;
- toute information bloquante ou présentant une difficulté technique d'acheminement à son destinataire peut être isolée, le cas échéant supprimée.

L'université informe l'utilisateur que le système d'information peut faire l'objet d'une surveillance et d'un contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Conformément à la décision du conseil du numérique du 21 octobre 2024, les audits de sécurité des réseaux, des services applicatifs, des annuaires Active directory, ...sont réalisés régulièrement.

Les personnels chargés des opérations de contrôle sont soumis au secret professionnel.

## 3.4 Protection antivirale

L'université a déployé une protection logicielle généralisée non seulement sur les serveurs, mais aussi les postes de travail des utilisateurs.

Le but d'un antivirus est de protéger toutes les machines du parc contre les attaques provoquées par des codes malveillants. Sur chaque poste utilisateur est installé un client antivirus. Il est interdit, par la présente charte, de désactiver, d'altérer le fonctionnement, ou de désinstaller ce client. Il est aussi interdit d'utiliser d'autres logiciels (antivirus ou autres) susceptibles d'entraîner un dysfonctionnement de l'antivirus installé en exécution de la stratégie de sécurité de l'université.

L'utilisation à des fins professionnelles d'un matériel autre que celui mis à disposition de l'utilisateur par l'université, notamment un matériel personnel, doit se faire dans le strict respect des principes de sécurité rappelés dans la présente charte.

Il appartient donc à l'utilisateur qui souhaite accéder aux ressources du système d'information de l'université de veiller à la sécurité du matériel qu'il utilise et à son innocuité.

Cette obligation incombe également aux membres du personnel qui utilisent un matériel informatique mis à disposition par l'établissement tout en en étant pleinement administrateurs, que cet état de fait soit motivé par la nécessité professionnelle ou tout autre facteur.

L'accès aux applications métiers (SIFAC, SIHAM, …) est interdit à partir d'un ordinateur personnel. Seul un ordinateur mis à disposition par l'université pourra bénéficier de ces accès.

# Article 4. Communications électroniques

## *4.1 Messagerie électronique*

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de l'université. C'est pourquoi une charte de messagerie est annexée. Cette charte est complétée par le guide pratique de l'utilisateur, qui présente un ensemble de règles impératives et de recommandations concernant la messagerie électronique dont le respect garantit la conservation de ces données.

## *4.2 Internet*

L'utilisation de la technologie Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'université.

Il est rappelé que le réseau Internet est soumis à l'ensemble des règles de droit en vigueur.

L'université met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible.

Cet accès Internet est destiné à des usages professionnels : il peut constituer le support d'une communication privée telle que définie en section II.1, dans le respect de la réglementation en vigueur.

**Les utilisateurs sont informés qu'en considération de la mission éducative de l'établissement, la consultation volontaire et répétée de contenus à caractère pornographique depuis les locaux ou via les moyens numériques de l'université est proscrite.**

L'université se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes. L'utilisateur en est dans ce cas informé.

L'accès à Internet mis à disposition par l'université n'est autorisé qu'au travers des dispositifs sécurisés mis en place (portail captif, certificat EDUROAM…) Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans le guide d'utilisation annexé à la présente charte.

L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet, par le biais d'actions de formation ou de campagnes de sensibilisation.

### *4.3 Téléchargements*

Tout téléchargement de fichiers, notamment de sons ou d'images, doit s'effectuer dans le respect des droits de propriété intellectuelle tels que définis à l'article VI.

L'université se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information, tels les virus, les codes et scripts malveillants ou les programmes-espions, tout fichier susceptible d'altérer le bon fonctionnement du système d'information.

## Article 5. Traçabilité

L'université est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des données échangées (conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur…).

L'université se réserve le droit de mettre en place des dispositifs de traçabilité sur tous les outils et services numériques qu'elle met à la disposition des utilisateurs.

Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée, ce traitement de données est inscrit au registre des traitements de l'établissement.

Les utilisateurs sont informés que la durée légale de conservation des fichiers de journalisation est d'une année à partir de la date d'enregistrement.

## Article 6. Respect de la propriété intellectuelle

### Général

*L'institution rappelle que l'utilisation des moyens informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et, plus généralement, de tous tiers titulaires de tels droits.*

*En conséquence, chaque utilisateur doit :*

- utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur dans le strict respect des licences qui leur sont attachées ;
- s'abstenir de reproduire, copier, diffuser, modifier, sans avoir obtenu préalablement et personnellement le cas échéant, si requis, l'autorisation du ou des titulaires des droits de propriété intellectuelle.

### Dispositif anti-plagiat

Dans le cadre de sa démarche de mise en place d'outils de prévention et de détection du plagiat, l'université met à disposition de ses enseignants-chercheurs et enseignants un logiciel de détection de similitudes accessible depuis l'ENT. Ce service permet d'analyser des travaux rendus par les étudiants sous forme

numérique, pour repérer et identifier des paragraphes similaires à des textes disponibles en ligne ou dans les bibliothèques de référence et dont les sources ne seraient pas citées.

L'université informe ses étudiants que leurs productions (rapport de stage, mémoire, thèse, etc.) sont susceptibles d'être analysées par la solution de détection de similitudes.

Un acte de plagiat peut constituer le délit de contrefaçon engageant la responsabilité civile, voire pénale, du plagiaire par infraction à la réglementation en matière de propriété intellectuelle. Cette pratique constitue également une infraction au règlement des examens de l'université, passible de sanctions disciplinaires pour fraude aux examens, décidées par la section disciplinaire compétente conformément aux dispositions du code de l'éducation (articles R712-9 à R712-46 et R811-11).

Les utilisateurs du numérique s'engagent sur l'honneur au respect de la réglementation en matière de propriété intellectuelle, ainsi qu'au respect des règlements intérieurs de l'université.
*Voir également l'annexe juridique : l'exception pédagogique en matière de droit d'auteur.*

### Usage de l'intelligence artificielle (IA)

L'intelligence artificielle (IA), et notamment les outils d'IA générative tels que les assistants conversationnels, les générateurs de textes, d'images ou de code, peuvent constituer des supports pédagogiques intéressants s'ils sont utilisés de manière encadrée et responsable.

L'université reconnaît le potentiel de ces technologies dans l'aide à la compréhension, à la révision, à la créativité ou encore à la recherche documentaire, sans toutefois ignorer les risques induits par leur usage non maîtrisé. Leur usage ne saurait se substituer au travail personnel attendu dans les évaluations, les mémoires ou les productions intellectuelles.

Les étudiants sont tenus de :

- respecter les consignes spécifiques données par leurs enseignants concernant l'usage d'outils d'IA ;
- ne pas utiliser l'IA pour produire un travail présenté comme entièrement personnel sans en indiquer clairement la source et la nature de l'assistance ;
- veiller à la **vérification critique des contenus générés**, qui peuvent comporter des erreurs, des approximations ou des biais ;
- respecter les règles relatives au **plagiat, à l'originalité des travaux et à l'honnêteté académique**.

L'usage inapproprié de l'IA dans un contexte académique pourra être considéré comme une **fraude ou tentative de fraude**, et faire l'objet de sanctions disciplinaires conformément au règlement intérieur de l'établissement.

## Article 7. Protection des données à caractère personnel

L'utilisateur est informé de la nécessité de respecter la réglementation en matière de traitements (automatisés ou non) de données à caractère personnel, conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et à la loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée.

Une donnée à caractère personnel est toute information relative à une personne physique susceptible d'être identifiée directement ou indirectement.

Tout traitement impliquant des données à caractère personnel doit être conforme aux dispositions du RGPD et de la loi n°78-17 du 6 janvier 1978 dite « informatique et libertés » modifiée. Sont notamment considérées comme des traitements les opérations suivantes : l'enregistrement, la conservation, la diffusion de données à caractère personnel sur support numérique ou papier. Sont également soumis à la réglementation les systèmes de vidéosurveillance.

En conséquence, tout utilisateur souhaitant procéder à un tel traitement devra en informer préalablement le délégué à la protection des données (DPO) qui prendra les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès, de rectification et d'opposition relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information. L'utilisateur dispose également d'un droit à la limitation du traitement et à la portabilité de ses données.

Ces droits s'exercent auprès du délégué à la protection des données (DPO) de l'université dpd@ube.fr

## *7.1 Registre des activités de traitement et transparence sur les traitements*

L'université s'engage à ce que les traitements de données personnelles soient mis en œuvre conformément à la réglementation en vigueur.
Ainsi, tout traitement de données personnelles doit être inscrit au registre des activités de traitement d'Université Bourgogne Europe.
Préalablement à la mise en œuvre de tout traitement de données personnelles, les personnes concernées sont informées :

- du responsable du traitement et des objectifs du recueil de ces données (finalités) ;
- de la base juridique du traitement de données personnelles ;
- du caractère obligatoire ou facultatif du recueil des données personnelles et de la liste des catégories de données traitées ;
- des catégories de personnes concernées ;
- des destinataires des données ;
- de la durée de conservation des données ;
- des mesures de sécurité (description générale) ;
- de l'existence éventuelle de transferts de données hors de l'Union européenne ou de prises de décision automatisées ;
- de leurs droits Informatique et Libertés et de la façon de les exercer auprès de l'université.

Ces informations doivent apparaître sur tout support de collecte de données personnelles (formulaires, etc.).

## *7.2 Finalité des données personnelles collectées*

Conformément aux principes de minimisation et de proportionnalité, Université Bourgogne Europe s'engage à ne traiter que les données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

L'université s'engage à ne pas traiter les données pour d'autres finalités que la finalité initiale, sauf à en informer la personne concernée et à recueillir son consentement préalable à la nouvelle finalité.

### *7.3 Confidentialité des données personnelles*

L'université s'assure que seules les personnes ayant besoin d'en connaître ont accès aux données personnelles des utilisateurs.
Toutes les personnes ayant accès aux données personnelles sont liées par un devoir de confidentialité et s'exposent à des mesures disciplinaires et/ou sanctions pénales si elles ne respectent pas ces obligations.
Toutefois, il conviendra de noter que les données peuvent être divulguées à des tiers autorisés en application d'une loi, d'un règlement ou en vertu d'une décision d'une autorité réglementaire ou judiciaire compétente.

### *7.4 Durée de conservation des données*

Les données sont stockées et conservées pour la durée nécessaire à la réalisation de la ou des finalité(s) visée(s) et conformément aux réglementations en vigueur applicables.

## Article 8. Limitation des usages

En cas de non-respect, par un utilisateur, des règles définies dans la présente charte, de ses annexes et des modalités présentées dans le guide pratique, le Président, ses délégataires, ou les RSSI pourra, après en avoir averti l'intéressé et sans préjuger des poursuites ou procédures de sanction pouvant être engagées à son encontre, limiter ou faire limiter les usages par mesure conservatoire :

- limiter les accès de l'utilisateur ;
- déconnecter l'utilisateur, avec ou sans préavis selon la gravité de la situation ;
- retirer les codes d'accès ou autres dispositifs de contrôle d'accès et fermer les comptes ;
- effacer, compresser ou isoler toute donnée ou tout fichier trop lourd, ou manifestement en contradiction avec la charte, ou qui mettrait en péril la sécurité des ressources ;
- interdire à l'utilisateur tout accès aux ressources dont il est responsable ;
- déconnecter du matériel sur le réseau UBE et le placer sous séquestre.

Tout abus dans l'utilisation à des fins extra-professionnelles des ressources mises à la disposition de l'utilisateur est passible des sanctions détaillées dans l'annexe juridique de la présente charte.

## Article 9. Usage raisonné et responsable du numérique

L'université encourage une utilisation **responsable, durable et éthique** du numérique, en cohérence avec ses engagements en matière de **transition écologique** et de **responsabilité sociétale**.

Les étudiants, enseignants et personnels sont invités à :

- adopter des **pratiques numériques sobres**, en évitant les usages excessifs ou inutiles (stockage superflu, envois massifs de courriels, usage abusif de la vidéo HD, etc.) ;
- **Privilégier les outils mutualisés** (plateformes collaboratives, partages de fichiers en ligne sécurisés) pour limiter l'empreinte environnementale ;
- éteindre les appareils électroniques lorsqu'ils ne sont pas utilisés et favoriser les équipements à faible consommation énergétique ;
- trier et supprimer régulièrement les fichiers et courriels inutiles afin de réduire le volume de données stockées ;
- être sensibilisés à l'impact environnemental du numérique, notamment en ce qui concerne la **consommation énergétique des datacenters**, des ordinateurs et des réseaux.

L'université s'engage à accompagner la communauté universitaire dans l'adoption de ces pratiques, à travers des actions de formation, de sensibilisation et des outils adaptés.

## Article 10. Annexe et Entrée en vigueur de la charte

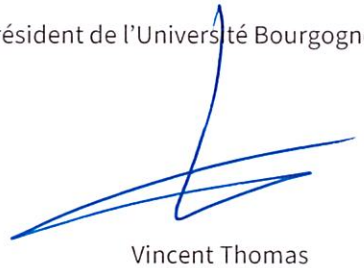
Sont annexés à cette charte **1 – Document principal,** les documents suivants :

2 – Guide pratique de l'utilisateur définissant les principales pratiques d'usage
3 – Charte de la messagerie
4 – Annexe juridique qui rappelle les dispositions législatives en vigueur
5 – Charte de déontologie des administrateurs système d'information
6 – Charte des organisations syndicales (fixant les principes et les modalités de l'utilisation, par les organisations syndicales, des technologies de l'information et de la communication, au sein de l'université, pour leur permettre de communiquer des informations syndicales sous forme dématérialisée) ;
7 – Charte intelligence artificielle (IA)

*L'ensemble de ces documents est accessible sur l'ENT de l'UBE.*

*La présente charte a valeur de règlement intérieur pour ce qui concerne l'usage des systèmes d'information.*
*Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des systèmes d'information.*

Président de l'Université Bourgogne Europe



Vincent Thomas

# CHARTE DE BON USAGE DES MOYENS NUMÉRIQUES DE L'UNIVERSITÉ BOURGOGNE EUROPE

*2 – Guide de bonnes pratiques*

## S'applique à :

Tout personnel, étudiant et usager du système d'information de l'Université Bourgogne Europe (UBE)
Ci-dessous désignés par l'« utilisateur »

## Par :

L'Université Bourgogne Europe
Ci-dessous désignée par « l'Université » ou « UBE »

**Document présenté au CSA du 11/06/2025**

**Document voté par le conseil d'administration de l'Université Bourgogne Europe le 08/07/2025. Ce document vaut pour règlement intérieur.**

ENT : Environnement Numérique de Travail

**https://ent.ube.fr**

## Préambule

Le présent guide pratique de l'utilisateur a pour objet d'accompagner les personnes autorisées à accéder au système d'information de l'université dans la mise en œuvre des règles de sécurité et de comportement préconisées par la charte de bon usage des moyens numériques.

Avec la charte, le présent guide complète le règlement intérieur régissant l'usage des moyens numériques que l'université met à disposition de ses utilisateurs.

Les utilisateurs sont informés que la violation des prescriptions du présent guide peut entraîner des sanctions. La nature des sanctions encourues est précisée dans l'annexe juridique de la charte.

La charte et les documents qui la complètent, tels l'annexe juridique et le présent guide de l'utilisateur, peuvent être consultés dans l'environnement numérique de travail de l'université.

Rappels :

- Que sont les « moyens numériques » ?

Les moyens numériques de l'université sont définis, par l'article I. al. 2 de la charte des bons usages, comme *« l'ensemble des logiciels et matériels, outils informatiques et services numériques, que l'université met à disposition de ses utilisateurs ».*

- Qui sont les « utilisateurs » ?

La notion d'« utilisateurs » est définie par l'article I. al. 3 de la charte comme *« l'ensemble des personnes ayant obtenu l'autorisation d'accéder au système d'information de l'université ».*

# SOMMAIRE

# 1. Règles de Sécurité

## *Gestion des comptes*

**Par mesure de sécurité, le compte informatique sera désactivé en cas d'inactivité pendant trois mois. L'utilisateur pourra réactiver seul sans intervention technique de la part de la direction du numérique (conseil du numérique du 21 octobre 2024).**

**Processus de blocage et déblocage.**

**En cas de problème de sécurité avéré ou en cas de suspicion de problème de sécurité, le compte informatique pourra être bloqué sans préavis, automatiquement ou manuellement par les services numériques de l'UBE. En cas de blocage, une information pourra être envoyée sur l'adresse de récupération associée au compte, à son informaticien de proximité.**

**Le compte sera débloqué après analyse et remédiation du problème source par l'informaticien de proximité ou, à défaut, par la Direction du Numérique.**

## *Gestion des mots de passe*

Chaque utilisateur doit veiller au respect de la sécurité liée aux mots de passe permettant l'accès à son environnement de travail (logiciels métiers …).

Un bon mot de passe est long, constitué de 12 caractères alphanumériques au minimum, avec des caractères spéciaux. Cette taille pourra être revue à la hausse en fonction des recommandés de la CNIL. Que la taille des mots de passe peut évoluer en fonction des recommandations de la CNIL, qui peut donner lieu à une délibération J.O. Il doit être unique et différent pour chaque compte. Le mot de passe de l'UBE ne doit jamais être utilisé pour d'autres sites. Chaque utilisateur est personnellement responsable des mots de passe qu'il a choisis.

Concrètement, chaque utilisateur doit :

- choisir un mot de passe robuste et n'ayant aucun lien avec son environnement familier ;
- veiller à la confidentialité de son mot de passe et notamment s'abstenir de l'écrire sur un support facilement accessible ;
- s'abstenir de réutiliser ce mot de passe ailleurs que sur son compte informatique UBE ;
- changer immédiatement son mot de passe en cas de doute sur sa confidentialité ;
- le mot de passe devra être modifié régulièrement suivant les recommandations du Conseil du Numérique du 21 octobre 2024. Un paramétrage interdit le réemploi d'un mot de passe déjà utilisé ;
- Ne jamais stocker des mots de passe dans les navigateurs (un coffre-fort électronique est mis à disposition des utilisateurs par l'UBE.

## *Paramétrage des postes de travail*

### a) Principes généraux

Le poste de travail de l'utilisateur constitue un outil qui doit être protégé des intrusions. À cet égard, il est conseillé, à chaque fois que cela sera possible :

- de paramétrer la mise en veille automatique de l'ordinateur avec demande du mot de passe pour son activation après une période d'inactivité ;
- d'effectuer systématiquement une déconnexion des serveurs réseau et de clore les applications actives avant de quitter son poste de travail.

### b) Protections logicielles : antivirus et pare-feu (« firewall »)

Un antivirus est un logiciel de protection dont le but est de détecter les logiciels malveillants (comme les virus, les « vers » ou les « chevaux de Troie »). Pour cela, il inspecte la mémoire, les disques durs de l'ordinateur et les volumes amovibles (CD, DVD, clé USB, disque dur externe...) pour vérifier que les fichiers présents ne contiennent pas de code malveillant connu. Il permet aussi d'effectuer régulièrement des analyses planifiées.

Un antivirus protège contre les codes malveillants qu'il connaît ou qu'il reconnaît. Il est donc non seulement indispensable d'utiliser un logiciel antivirus, mais aussi de veiller à sa mise à jour.

Un pare-feu ou « firewall » permet de protéger l'ordinateur connecté à Internet des attaques externes initiées par des programmes ou des personnes malveillants.

Ces mesures de protection sont mises en place par la direction du numérique et les informaticiens de composantes sur les postes informatiques qu'ils gèrent ; elles sont à la charge de l'utilisateur pour les équipements dont il est administrateur.

### c) Mises à jour

Les logiciels, comme toute création humaine, comportent des défauts. Parmi ces défauts, on en trouve qui porte atteinte à la sécurité ; ils sont appelés « vulnérabilités ». Au quotidien, de nombreuses vulnérabilités sont découvertes dans les systèmes d'exploitation et les logiciels équipant les matériels informatiques. Ces failles sont très rapidement exploitées par les pirates les plus expérimentés pour tenter de prendre le contrôle ou de voler des informations sur les postes de travail et les serveurs.

Il est donc primordial d'appliquer systématiquement les mises à jour de sécurité, au fur et à mesure de leur publication. Cette maintenance est assurée par la direction du numérique et par les informaticiens de composantes pour les postes informatiques qu'ils gèrent ; elle est à la charge de l'utilisateur pour les équipements dont il est administrateur.

### d) Les accessoires du poste de travail, dont les périphériques de stockage

Les périphériques et particulièrement les périphériques de stockage comme les clés USB, les disques durs externes, les cartes mémoire - voire les téléphones portables ou baladeurs qui offrent

cette fonctionnalité - sont un vecteur de plus en plus utilisé pour infecter les postes de travail.

Un périphérique de stockage d'origine inconnue peut non seulement contenir des virus, mais également être configuré pour « aspirer » le contenu du poste de travail à l'insu de l'utilisateur. Il est donc interdit d'utiliser un matériel d'origine inconnue, particulièrement pour un échange de données.

Par conséquent, il est interdit d'utiliser des périphériques de stockage (clé USB, disque dur externe, NAS …) professionnels ou privés (conseil du numérique du 21 octobre 2024) notamment sur les postes des agents administratifs qui ont un accès aux applications métiers (SIFAC, SIHAM, …).

Les membres du personnel de l'université autorisés à exercer leurs missions en télétravail veilleront à appliquer cette recommandation avec une particulière vigilance.

Les échanges de données devront s'effectuer via les serveurs de stockage mis à disposition par l'université. Dans des cas exceptionnels où l'échange de données ne peut s'effectuer via ces outils, l'utilisation de périphériques externes pourra être tolérée.

### e) Utilisation du poste en mode administrateur

Un compte ayant les droits « administrateur » offre à son titulaire un contrôle très étendu sur les logiciels équipant le poste informatique. Les comptes administrateurs sont ainsi les cibles privilégiées de nombreux programmes malveillants tentant d'accéder aux ressources du poste.

Il est vivement recommandé d'utiliser au quotidien - et en particulier pour naviguer sur Internet - un compte ne possédant pas les privilèges « administrateur ».

D'une manière générale, l'attention des personnels disposant de ces privilèges sur un poste informatique est attirée sur leur responsabilité dans la gestion des mises à jour et la surveillance des alertes émises par les dispositifs de protection antivirale. Les utilisateurs des postes permettant l'accès aux applications de gestion (SIFAC, SIHAM, …) ne pourront pas avoir des droits administrateur sur leur poste.

L'utilisation de logiciels de prise de contrôle à distance (Teamviewer, LogMein) est interdite. Il faut se reporter sur les alternatives sécurisées mises en place et prévoir une procédure de dérogation pour des situations exceptionnelles (Conseil du numérique du 21 octobre 2024).

L'utilisation de VPN tiers est proscrite, il faut utiliser les solutions sécurisées proposées par la direction de l'université et disponible pour toutes les entités (Conseil du numérique du 21 octobre 2024).

## *Navigation sur Internet (Web)*

Il est rappelé que l'accès à Internet n'est autorisé qu'au travers des dispositifs sécurisés mis en place par l'université.

Certains sites malveillants profitent des failles des navigateurs pour récupérer les données

présentes sur le poste de travail. D'autres sites mettent à disposition des logiciels qui, sous une apparence anodine, peuvent prendre le contrôle de l'ordinateur et transmettre son contenu à des tiers, à l'insu de son utilisateur.

La prudence est recommandée avant tout téléchargement, particulièrement pour les utilisateurs qui disposent des privilèges d'administrateur de leur poste. Les utilisateurs doivent s'abstenir de se connecter à des sites suspects et éviter de télécharger des logiciels dont l'innocuité n'est pas garantie ; par exemple : vérifier la pérennité du logiciel et/ou la nature de l'éditeur.

## *Sauvegarde de données : quelques repères*

La sauvegarde doit être organisée sur tout type d'appareil utilisé à titre professionnel, du poste informatique fixe au matériel nomade.

La Direction du numérique organise une sauvegarde des données sur l'ensemble des serveurs qu'elle gère, et notamment pour les services de stockage (serveurs de fichier, CLOUD, GED).

Les données professionnelles ne devront pas être stockées en local sur les disques durs des postes. Elles seront stockées sur les outils de stockage mis à disposition par la direction du numérique qui se charge de la sauvegarde de ces données.

Pour tous les autres, une sauvegarde régulière par chaque utilisateur est l'unique moyen de garantir la pérennité des données et de se prémunir contre les conséquences néfastes d'un problème technique, d'une attaque informatique ou d'un vol.

## *Messagerie électronique*

De manière générale, il est déconseillé d'ouvrir des fichiers en provenance d'un expéditeur inconnu. Cette prescription concerne en particulier les fichiers compressés ou exécutables dont l'ouverture peut notamment générer l'activation de virus informatiques, de codes malveillants, susceptibles d'entraîner des conséquences d'une extrême gravité pour l'université. La messagerie électronique véhiculant de nombreux courriels frauduleux ou falsifiés, en particulier les phishings ou hameçonnages, il convient d'être particulièrement prudent avant de suivre une consigne (« cliquez ici », « répondez à ceci », « faites cela ») figurant dans un courriel et au besoin de vérifier par un autre canal (demande à un collègue ou un informaticien) la légitimité du contenu d'un message.

Pour tout courriel douteux, le transmettre à spaminfo@ube.fr.

Les utilisateurs sont informés que l'université se réserve le droit de retenir, d'isoler et/ou de supprimer tout message à l'aide de moyens automatisés, et ce, sans que ces messages aient été nécessairement ouverts, afin de s'assurer de leur innocuité.

Les utilisateurs sont informés que tout message bloquant ou présentant une difficulté technique d'acheminement à son destinataire peut être détruit sur décision de la direction du numérique.

Les administrateurs du système d'information sont autorisés, en cas de difficultés majeures, à arrêter les services réseaux.

### *Règles de sécurité en cas de déplacement à l'étranger*

Le passeport de conseils aux voyageurs édité par l'ANSSI énonce les bonnes pratiques de sécurité numérique à observer lorsqu'un agent se déplace à l'étranger avec un téléphone, une tablette, un ordinateur …

Il est disponible sur le site de l'ANSSI et sur l'intranet UBE.

Les principales recommandations sont les suivantes :

- utilisez de préférence du matériel dédié aux missions (ordinateurs, téléphones ...) Ces appareils ne doivent contenir aucune information autre que celles dont vous avez besoin pour la mission ;
- sauvegardez les données que vous emportez et laissez la sauvegarde en lieu sûr. Vous récupérerez ainsi vos informations à votre retour en cas de perte, de vol ou de saisie de vos équipements ;
- évitez de partir avec des données sensibles ;
- utilisez un filtre de protection-écran pour votre ordinateur ;
- marquez vos appareils d'un signe distinctif (comme une pastille de couleur).

## 2. Du bon usage de la messagerie électronique

### *Principes généraux*

Un diagnostic fait à la demande du CHSCT a révélé en juin 2014 que la messagerie électronique participe à la dégradation des conditions de travail et peut-être source de risques psychosociaux (RPS).

Dans un souci de prévention et d'amélioration de la qualité de vie au travail, le CHSCT recommande les bonnes pratiques suivantes :

- les menaces pour la confidentialité des données et la sécurité informatique (se reporter à la section I du présent document) ;
- son impact écologique, lié au volume - nombre et poids - des messages transmis (se reporter à la section V du présent document) ;
- son impact sur la qualité de vie au travail.

Une utilisation raisonnée de la messagerie s'impose pour répondre à ces enjeux : la nécessité de restreindre l'usage de la messagerie électronique aux échanges professionnels, de limiter l'envoi des pièces jointes, de circonscrire au strict nécessaire le nombre de destinataires d'un message :

- l'envoi collectif massif d'un message peut être source de RPS. Il est recommandé de ne pas en abuser et de vérifier la pertinence des destinataires ;
- l'envoi d'un message agressif ou polémique peut être générateur de souffrance. Il est recommandé de prendre conscience de son impact éventuel ;
- la réception d'un message en dehors des heures de travail peut être source de stress ;

- nous recommandons vivement l'application de la règle "trois courriels" qui stipule qu'après trois courriels conflictuels, d'arrêter les échanges numériques, et privilégier un échange téléphonique ou présentiel.

## *Rappel concernant les messages à caractère privé*

Aux termes de la charte de bon usage des moyens numériques, le terme « professionnel » vise les usages n'ayant pas un caractère strictement privé. Le caractère privé n'est reconnu qu'aux actes détachés de l'exercice des missions confiées (pour les enseignants-chercheurs, les enseignants et le personnel administratif, technique de l'université) ou détachés des activités pédagogiques (pour les utilisateurs étudiants).

Tout message à caractère strictement privé, reçu ou émis, doit comporter en objet la mention « Privé », afin d'exprimer sans ambiguïté le caractère extra-professionnel du message.

Les messages ne comportant pas, en objet cette mention ou n'étant pas classé dans un répertoire nommé privé sont réputés professionnels.

## *Caractéristiques et limitations de la messagerie électronique*

L'envoi de messages contenant des pièces jointes est une pratique énergivore, ayant un fort impact environnemental, coûteuse en termes de ressources et potentiellement dangereuse pour le poste de travail. Les utilisateurs veilleront à ne l'utiliser qu'en cas de nécessité, en privilégiant pour leurs usages courants les outils collaboratifs et de partage sécurisé proposés par l'université.

Pour prévenir les abus, les messages émis ou reçus font l'objet d'une limitation technique de leur taille. En cas de dépassement de la taille limite, le message est rejeté et l'émetteur reçoit un message de non-distribution.

Par ailleurs, l'envoi de message à un grand nombre de destinataires doit être proscrit. Cette pratique provoque le ralentissement des serveurs de messagerie de l'établissement. Surtout, les fournisseurs externes de services de messagerie assimilent ces messages à des pourriels ou « spams » et, en conséquence, placent l'université sur une liste noire. Ceci entraîne le blocage, chez ces fournisseurs, de tous les messages en provenance de l'université.

Pour prévenir de tels dysfonctionnements, une limite technique est mise en œuvre par la direction du numérique : en cas d'abus, le compte de l'expéditeur est bloqué.

S'il est nécessaire de diffuser des messages à de très nombreux destinataires, il est impératif d'utiliser les listes de diffusion (et notamment le service Sympa), qui ne provoquent aucune perturbation.

## *Stockage et archivage des messages électroniques*

L'utilisateur doit mettre en œuvre les moyens nécessaires à la conservation des messages qui

pourraient être indispensables à son activité.

La messagerie des personnels de l'université est sauvegardée quotidiennement, ce qui ne dispense en aucun cas les utilisateurs de procéder à un archivage personnel. En procédant ainsi, les usagers peuvent plus facilement purger leurs boîtes de messagerie et, par conséquent, réduire concrètement leur impact environnemental.

Chaque utilisateur doit en conséquence organiser lui-même la conservation de ces éléments en décidant :

- du nombre de sauvegardes et de leur périodicité ;
- du choix des fichiers et messages conservés et de ceux qui sont détruits ;
- de la méthode et de la durée de stockage.

Chaque utilisateur dispose d'une certaine volumétrie (quota) pour sa boite de messagerie sur les serveurs de l'université. En cas de remplissage complet de la boite, les messages ne pourront plus être délivrés dans la boite de l'utilisateur et pourront être perdus, c'est pourquoi nous recommandons un tri régulier ainsi que la mise en place d'un archivage local des messages.

# 3. Du bon usage du matériel informatique mis à disposition par l'établissement

## *Principes généraux*

L'établissement définit la politique d'acquisition et de gestion des équipements numériques mis à disposition des membres de son personnel.
Les grandes lignes de cette politique sont les suivantes :

- Les agents administratifs ne doivent pas utiliser deux ordinateurs en parallèle (par exemple : un ordinateur fixe et un ordinateur portable). Ce principe ne peut connaître que de rares exceptions, dûment motivées : la gestion d'un double parc informatique est impossible à assumer ;
- Tout matériel informatique acquis avec des deniers publics est intégré dans l'inventaire physique et reste l'entière propriété de l'université. Lors de l'installation d'un nouveau poste portable ou fixe, l'ancien est repris. Il sera réutilisé si possible, donné ou détruit selon une procédure écoresponsable.

## *Équipements nomades*

Lorsqu'un équipement nomade, de type appareil photo numérique, caméscope, téléphone mobile, ordinateur portable ou tablette, est confié à un utilisateur de l'université, cette mise à disposition :

- est réputée intervenir dans le cadre exclusif des activités professionnelles du bénéficiaire ;
- entraîne l'obligation pour le bénéficiaire d'apporter tous les soins nécessaires à la bonne conservation de ce matériel.

Par exemple, le bénéficiaire doit veiller particulièrement à :

- ne pas altérer sa configuration logicielle ;
- ne pas exposer l'équipement confié à la chaleur ni à l'humidité ;
- ne pas le laisser sans surveillance ;
- ranger le matériel non utilisé dans un endroit sécurisé.

Pour des raisons de sécurité, l'accès au réseau filaire des bâtiments de l'établissement est réservé au matériel confié par l'université, aucun autre matériel ne doit y être connecté.

### *Vol / Perte*

En cas de vol de l'équipement confié, une déclaration doit être effectuée sans délai auprès des RSSI ( rssi@ube.fr) en précisant les données stockées sur l'ordinateur. S'il s'agit de données sensibles, les RSSI procèderont au dépôt de plainte.

Toute fausse déclaration est passible de sanctions disciplinaires et/ou de poursuites pénales.

En cas de perte ou de vol de l'équipement confié, une déclaration détaillée doit être adressée à l'université par l'intermédiaire de Helpdesk.

### *Détérioration*

En cas de détérioration du matériel nomade prêté, celui-ci doit être restitué au responsable de l'université qui a autorisé le prêt, avec un descriptif des dommages constatés et un exposé des circonstances à l'origine de la détérioration.

## 4. Conduite à tenir en cas d'absence, de départ ou de mutation

### *Principes généraux*

Aux termes de l'article II.2 de la charte de bon usage des moyens numériques, il appartient à tout membre du personnel, quittant à titre provisoire ou définitif l'université, de respecter deux obligations :

- permettre l'accès à ses données professionnelles en vue de garantir la continuité de service ;
- procéder à la suppression des données privées qu'il aurait stockées dans le système d'information.

Par ailleurs, il va de soi que les matériels mis à disposition pour l'exercice d'une mission (se reporter à la section III du présent document) doivent être restitués à l'issue de celle-ci.

### *Suppression des données privées*

L'attention des agents et des enseignants de l'université est attirée sur la nécessité de prendre en charge personnellement la récupération puis la suppression des données privées qu'ils auraient stockées dans le système d'information de l'établissement.

En conséquence, l'université ne peut être tenue responsable :

- de la perte des données qui n'auraient pas été récupérées par l'utilisateur avant son départ ;
- de la divulgation ultérieure de données qu'il n'aurait pas supprimées.

### *Préparer son absence*

Au-delà de la suppression des données privées, il incombe également au supérieur hiérarchique de l'agent qui s'apprête à quitter l'établissement de :

- demander la suppression des accès aux logiciels, applications de travail (SIFAC, …) ;
- faire retirer l'adresse électronique professionnelle des différentes listes de diffusion ;
- s'assurer que l'agent en question aura mis en place un « répondeur » sur sa messagerie électronique, afin d'orienter les demandeurs vers un autre contact, au plus tard le jour de son départ effectif.

## 5. Prise en compte des enjeux environnementaux et sociétaux

### *Principes généraux*

La mise en œuvre d'une stratégie transversale en matière de développement durable et de responsabilité sociétale est au cœur des objectifs de l'université.

### *Consommation d'énergie*

Pour limiter la consommation d'énergie, il est recommandé de paramétrer la mise en veille automatique de vos appareils au bout d'un certain temps d'inactivité, lorsque cela est possible.

Toutefois, lorsque les équipements ne sont plus utilisés, la seule mise en veille est insuffisante. Il est alors recommandé de :

- éteindre vos écrans de bureau lorsque vous partez en réunion, et en fin de journée ;
- éteindre vos ordinateurs en fin de journée ;
- éteindre les imprimantes et les copieurs en fin de semaine.

## *Gestion des impressions*

Compte tenu de l'impact environnemental des équipements concernés, l'attention des utilisateurs est attirée sur les bonnes pratiques en matière de gestion des impressions.

### a) Concernant le matériel fourni par l'établissement :

L'université privilégie la mise à disposition de copieurs partagés. L'utilisation d'imprimantes individuelles ou "imprimantes de bureau" est exceptionnelle et limitée à des besoins spécifiques.

### b) Concernant les usages :

Le recours à l'impression d'un document doit répondre à un besoin avéré de l'utilisateur. Les impressions recto verso doivent être privilégiées, à chaque fois que c'est possible.

Comme pour tous les services numériques de l'établissement, ces équipements ne doivent être utilisés qu'à des fins professionnelles.

## *Bonnes pratiques en matière de stockage*

Il est recommandé de faire régulièrement « le ménage » dans les données stockées localement et en ligne, en supprimant les fichiers qui ne sont plus utiles et ne nécessitent pas d'être archivés. À ce titre, il est notamment demandé de :

- purger régulièrement le contenu du dossier téléchargement du système d'exploitation, ainsi que celui des corbeilles (système et messagerie) ;
- purger régulièrement les bibliothèques et répertoires partagés en éliminant les versions intermédiaires des fichiers et documents qui y sont enregistrés.

## *Utilisation responsable de la bande passante*

Tout moyen permettant de limiter la bande passante consommée par un ordinateur contribue à réduire l'impact environnemental de nos usages numériques. À ce titre, il est notamment recommandé de :

- brider la résolution des vidéos consultées en ligne, lorsque cela n'est pas préjudiciable à leur bonne compréhension ;
- enregistrer les sites Web consultés fréquemment dans ses favoris et ainsi éviter de passer par un moteur de recherche ;
- gérer sa messagerie électronique de manière raisonnée et limiter le poids des messages envoyés (se reporter à la section II du présent document).

## *Accessibilité des documents produits et diffusés*

Dans le cadre de leurs activités, tous les membres de la communauté universitaire sont amenés à produire ou à consulter des documents, que ceux-ci soient administratifs, scientifiques ou à visée pédagogique.

Il est essentiel de rendre ces documents accessibles à tous les usagers sans distinction aucune, en ayant une attention particulière pour les personnes en situation de handicap (Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées Article 47 et Décret n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne).

Par conséquent, il est requis que tout document essentiel aux activités des usagers de l'université soit conçu et diffusé de manière à faciliter son accès, notamment aux technologies d'assistance utilisées par les personnes en situation de handicap.

L'amélioration de l'accessibilité repose sur quelques principes et méthodes que les outils bureautiques facilitent grandement si on en connaît la teneur. Un ensemble de recommandations se trouvent dans le guide pour la création de documents accessibles mis à disposition par l'université. Une courte séance de sensibilisation aux éléments essentiels est également proposée dans le cadre de la formation continue des personnels (formation « Rendre accessibles les documents que vous créez »).

# 6. Formation

La formation de sensibilisation des usagers aux règles de sécurité informatiques est inscrite au plan de formation UBE. Il est conseillé à tout utilisateur de les suivre. Cette formation devient obligatoire pour tous les nouveaux arrivants à l'UBE (décision du conseil du numérique du 21 octobre 2024).

Suite à la décision du conseil du numérique du 21 octobre 2024, des campagnes de phishing ou de tentative d'attaque seront menées afin de sensibiliser les utilisateurs

# 7. Besoin d'aide ?

## *Assistance*

En cas de besoin d'assistance ou de renseignements complémentaires :

1. **Contactez les informaticiens de votre composante** pour une aide de proximité.
2. **Accédez à l'Environnement Numérique de Travail (ENT)** à l'adresse suivante : https://ent.ube.fr, puis cliquez sur l'onglet **« Assistance »** situé en haut de la page. Selon la nature de votre problème, vous pourrez :
    - Consulter la **FAQ** (Foire Aux Questions) ;
    - Déposer une demande d'assistance via le **HELPDESK** ;
    - Accéder à la section **« Compte compromis »** si vous suspectez une intrusion.
3. **Étudiants uniquement : un guichet unique** est également à votre disposition pour toute demande d'information ou de support, à l'adresse suivante : 📧 **guichet-unique@ube.fr**

## *Données à caractère personnel*

Le contact privilégié pour l'exercice des droits reconnus par la règlementation « Informatique et Libertés » et pour toutes questions relatives à la protection des données à caractère personnel est le délégué à la protection des données de l'université : dpd@ube.fr.

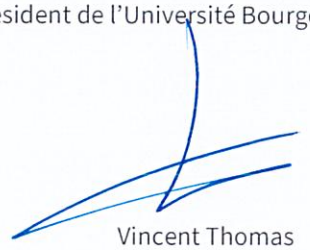
## *Mise à jour et disponibilité des documents de référence*

L'environnement numérique de travail recense les documents de référence mis à la disposition des utilisateurs de l'université.

La charte de bon usage des moyens numériques et l'intégralité de ses annexes – dont le présent guide pratique - sont consultables, dans leur dernière version, sur l'intranet.

***LE PRÉSENT GUIDE PRATIQUE FERA L'OBJET DE MISES À JOUR ET IL APPARTIENT À L'UTILISATEUR DE PRENDRE CONNAISSANCE DE TOUTE NOUVELLE VERSION QUI SERA PUBLIÉE SUR L'ENT.***

Président de l'Université Bourgogne Europe



Vincent Thomas

# CHARTE D'UTILISATION DE LA MESSAGERIE ÉLECTRONIQUE DE L'UNIVERSITÉ BOURGOGNE EUROPE

*3 – Messagerie électronique*

**S'applique à :**

Tout personnel, étudiant et usager du système d'information de l'Université Bourgogne Europe (UBE)
Ci-dessous désignés par l'« utilisateur »

**Par :**

L'Université Bourgogne Europe
Ci-dessous désignée par l'« université », UBE

**Mise à jour de la charte utilisation de la messagerie électronique votée en CA le 28 juin 2007.**

**Charte présentée au CSA du 11/06/2025**

**Votée par le Conseil d'Administration (CA) de l'université le 08/07/2025. Cette Charte vaut pour règlement intérieur en ce qui concerne l'usage de la messagerie électronique et des services associés.**

ZIMBRA : service de messagerie collaboratif de l'UBE

**Personnels :** https://webmail.u-bourgogne.fr/zimbra
**Étudiants :** https://etu.u-bourgogne.fr/zimbra

## Préambule

La fourniture des services liés aux technologies de l'information et de la communication s'inscrit dans la mission de service public de l'Enseignement supérieur. Elle répond d'une part à un objectif pédagogique et professionnel et d'autre part à une utilisation privative conformément aux dispositions en vigueur protégeant la vie privée (utilisation résiduelle).

Par cette offre, l'université met à disposition de ses utilisateurs un outil de travail utilisant les services électroniques de communication qui doit en particulier permettre d'améliorer la circulation de l'information au sein du système éducatif et de la rendre accessible à tous, de façon à renforcer la cohérence et l'efficacité de la démarche éducative et administrative.

La Charte précise tout d'abord son cadre légal. Elle rappelle notamment l'application du droit à internet afin de sensibiliser et de responsabiliser l'utilisateur.

Elle définit les droits et obligations que l'université s'engage à respecter et notamment les conditions et les limites des éventuels contrôles portant sur l'utilisation du service.

Cette Charte est spécifique à la messagerie électronique de l'université (courriels et listes de diffusion exclusivement). Elle est complémentaire à la Charte d'usage des Technologies de l'Information et de la Communication (TIC) de l'université à laquelle elle est annexée.

Elle rappelle l'existence de sanctions disciplinaires applicables en cas de contravention aux règles établies ou rappelées par la Charte.

# SOMMAIRE

**IL EST TOUT D'ABORD RAPPELÉ LA NÉCESSITÉ DE RESPECTER LA LÉGISLATION**

## Article 1. Respect de la législation

La quantité et la facilité de circulation des informations et des contenus sur internet ne doivent pas faire oublier la nécessité de respecter la législation. Internet et les réseaux de communication numériques ne sont pas des zones de non-droit.

Le rappel non exhaustif des règles de droit principalement concernées par l'utilisation d'internet et du service de messagerie proposé vise le double objectif de sensibiliser l'utilisateur à leur existence et à leur respect et de renforcer ainsi la prévention d'actes illicites.

Sont ainsi notamment (mais pas exclusivement) interdits et pénalement sanctionnés :

- l'atteinte à la vie privée d'autrui ;
- la diffamation et l'injure ;
- la provocation de mineurs à commettre des actes illicites ou dangereux, le fait de favoriser la corruption d'un mineur, l'exploitation à caractère pornographique de l'image d'un mineur, la diffusion de messages à caractère violent ou pornographique susceptibles d'être perçus par un mineur ;
- la provocation à la réalisation d'actes de terrorisme et à leur apologie ;
- l'incitation à la consommation de substances interdites ;
- la provocation aux crimes et délits et la provocation au suicide, la provocation à la discrimination, à la haine notamment raciale, ou à la violence ;
- l'apologie des crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité ; la négation de crimes contre l'humanité ;
- la contrefaçon de marque ;
- la reproduction, représentation ou diffusion d'une œuvre de l'esprit (par exemple : extrait musical, photographie, extrait littéraire …) ou d'une prestation de droits voisins (par exemple : interprétation d'une œuvre musicale par un artiste, phonogramme, vidéogramme, programme d'une entreprise de communication audiovisuelle) en violation des droits de l'auteur, du titulaire de droits voisins et/ou du titulaire des droits de propriété intellectuelle ;
- les copies de logiciels commerciaux pour quelques usages que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle.

**IL EST ENSUITE CONVENU CE QUI SUIT**

## Article 2. Description du service proposé

L'université offre à l'utilisateur, un service de messagerie électronique à usage « professionnel et personnel (vie privée résiduelle) », permettant d'établir une communication interne ou externe entre les différents utilisateurs, suivant les standards techniques en vigueur sur les réseaux de communication numérique.
L'université met à disposition des utilisateurs un Webmail (service de courriels en ligne).
On entend par Webmail un service de messagerie accessible sur internet qui permet l'émission et la manipulation de courriers électroniques.

# Article 3. Messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail et de mutualisation de l'information au sein de l'UBE.

La messagerie est un outil destiné à des usages professionnels : elle peut constituer le support d'une communication privée dans les limites définies à la section II.1.

### (a) Adresses électroniques

L'UBE s'engage à mettre à la disposition de l'utilisateur une boîte à lettres professionnelle nominative lui permettant d'émettre et de recevoir des messages électroniques.

Dans la mesure du possible, l'adresse électronique attribuée par l'administration à chaque personnel de l'UBE prend la forme prenom.nom@ube.fr, sauf cas particulier ou situations d'homonymie.

De la même manière, l'adresse électronique attribuée par l'administration aux étudiants de l'UBE prend, si possible, la forme prenom.nom@etu.ube.fr sauf cas particulier ou situations d'homonymie.

L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

Une adresse électronique, fonctionnelle ou organisationnelle, doit être privilégiée notamment si elle est exploitée par un service ou un groupe d'utilisateurs.

La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'«utilisateurs», relève de la responsabilité exclusive de l'UBE : ces adresses ne peuvent pas être utilisées sans autorisation explicite.

### (b) Contenu des messages électroniques

Les messages électroniques permettent d'échanger des informations à vocation professionnelle liées à l'activité de l'UBE. En toutes circonstances, l'utilisateur doit adopter un comportement responsable et respectueux des dispositions contenues dans la présente charte.

Par référence à l'article II, section II.1, tout message est réputé professionnel sauf s'il comporte en objet la mention "privé" ou s'il est stocké dans un espace spécifique de données identifié comme tel.

Les messages électroniques dont le contenu ou une partie du contenu comporte des mentions contraires aux bonnes mœurs ou portant atteinte à la vie privée ou à l'image d'autrui ou contrevenant au droit d'auteur sont interdits.

Les auteurs de messages contenant de telles mentions sont susceptibles de faire l'objet de poursuites pénales ainsi que de poursuites disciplinaires par l'établissement.

### (c) Émission et réception des messages

Pour garantir la confidentialité des données échangées, l'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.

Pour la même raison, il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en seront précisés dans le guide pratique de l'utilisateur.

Des recommandations concernant l'utilisation de la messagerie et la composition des messages sont présentées dans le guide pratique de l'utilisateur annexé à la présente charte ainsi que dans la charte sur la qualité de vie numérique.

### (d) Statut et valeur juridique des messages

Les écrits électroniques et notamment les messages électroniques échangés avec des tiers ont la même valeur que les écrits manuscrits.

### (e) Stockage et archivage des messages

Chaque utilisateur doit organiser et assurer la conservation des messages pouvant être indispensables à l'exercice de ses activités ou simplement utiles en tant qu'éléments de preuve.

Le guide pratique de l'utilisateur, annexé à la présente charte, présente un ensemble de règles impératives et de recommandations dont le respect garantit la conservation de ces données.

## Article 4. Définition de l'utilisateur

Les informations techniques ont été reportées dans le document « Détails techniques relatifs à la messagerie électronique ».

L'utilisateur est le bénéficiaire d'un accès aux services numériques et notamment au service de messagerie proposé par l'université, selon les informations techniques précisées dans le document « Détails techniques relatifs à la messagerie électronique ».

## Article 5. Droits d'accès et d'utilisation de l'utilisateur

Le moyen d'accès à la messagerie, mis à disposition de l'utilisateur est constitué d'un identifiant et d'un mot de passe strictement personnels, confidentiels et incessibles (ils ne doivent donc jamais être transmis à un tiers ni même à un supérieur hiérarchique). Il ne faut jamais répondre à un message électronique demandant ses codes d'accès, même si ce dernier peut paraître venir d'un service informatique de l'université d'une instance administrative ou juridique, il s'agit en fait d'une attaque de type hameçonnage (phishing).
Aucun personnel, aucune entité ou autorité administrative n'est autorisé ni habilité à demander ces informations.

4.1 - À l'exception des règles applicables aux boîtes de messagerie électronique fonctionnelles, le droit d'accès à la messagerie électronique est personnel, incessible et temporaire. Il fait l'objet d'un renouvellement annuel tacite.
L'accès disparaît éventuellement dans les cas prévus à l'article 10 et 11.

4.2 - Un utilisateur doctorant est avant tout un étudiant et dispose donc d'une adresse de messagerie étudiante en conséquence. Il peut également bénéficier d'une adresse en tant que personnel de l'université dès lors qu'il remplit les conditions de l'article 3.

4.3 - L'utilisateur peut demander à l'université la communication des informations à caractère personnel le concernant et les faire rectifier conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ou toute disposition légale ou réglementaire à venir ayant le même objet. En vertu des dispositions légales et réglementaires en vigueur, la remise de ces informations peut être ordonnée par voie de justice.

4.4 - L'utilisateur reconnaît que l'université n'exerce aucun contrôle (hors antispam et antivirus) sur le contenu des messages envoyés ou reçus dans le cadre de la messagerie électronique et l'accepte. L'université ne pourra, de ce fait, être tenue pour responsable des contenus échangés.

**4.5 - Pour des raisons de sécurité, les usagers ne pourront pas rediriger des adresses de messagerie en @ube.fr vers les messageries autres qu'internes ou celles des co-tutelles (Conseil du Numérique de 2024).**

4.6 - En cas de perte de ses codes d'accès, l'utilisateur peut récupérer l'accès aux services numériques et donc à sa messagerie en prenant contact avec le service adéquat qui lui sera indiqué par un informaticien de proximité. Une vérification d'identité sera effectuée avant toute opération permettant la restitution de l'accès aux services numériques.

# Article 6. Engagements de l'université

L'université fait bénéficier à toute personne remplissant les conditions ci-dessus définies à l'article 3 d'un accès au service qu'elle propose.

## *6.1 Obligations techniques et disponibilité du service*

Le service est conforme aux standards techniques de l'internet et aux normes en usage. La politique en place à l'université est détaillée dans le document « Détails techniques relatifs à la messagerie électronique ».

### Protection des données à caractère personnel de l'utilisateur

En application des dispositions de la loi informatique et Libertés n° 78-17 du 6 janvier 1978 modifié et de la législation en vigueur, l'université s'engage à respecter les règles légales de protection des données à caractère personnel. Elle garantit notamment à l'utilisateur :

- de n'utiliser les données à caractère personnel le concernant que pour les strictes finalités pour lesquelles elles sont nécessaires (ouverture du compte d'accès, contrôles techniques définis à l'article 5-4) ;
- de lui communiquer la destination des informations enregistrées et leur durée de conservation, laquelle ne peut en tout état de cause excéder ce qui est nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou traitées ;
- un droit d'accès aux données et de rectification le concernant.

### Conservation des traces

L'université archivera, pendant la durée préconisée par la loi, la date, les émetteurs et les destinataires de tout message ayant transité sur le système. Actuellement, cette durée est de 1 an.

Le contenu des messages (objet, corps du message, pièces jointes …) ne fera pas l'objet d'un archivage particulier sans l'autorisation de l'utilisateur (hors sauvegardes système).

### Contrôles techniques

L'université dispose des moyens techniques suivants pour procéder à des contrôles de l'utilisation de ses services :

- contrôle des volumes stockés ;
- contrôle des flux ;
- contrôle de sécurité ;

L'utilisateur accepte un contrôle a posteriori de l'utilisation de sa messagerie qui ne pourra porter que sur des indications générales de fréquence, de volume, de taille des messages, du format des pièces jointes, sans qu'il n'y ait aucun contrôle sur le contenu des messages échangés.
L'université garantit à l'utilisateur que seuls ces moyens de contrôle sont mis en œuvre.

Ces contrôles techniques sont justifiés :

- **soit par un souci de sécurité du réseau et/ou des ressources informatiques.**

Pour des nécessités de maintenance, de gestion technique et de sécurité de son réseau et de son système d'information, l'utilisation des services et notamment des ressources matérielles et logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment dans le respect des règles relatives à la protection de la vie privée et au respect des communications privées. L'université se réserve dans ce cadre le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système.

- **Soit par un souci de vérification que l'utilisation des services reste conforme aux objectifs rappelés dans le préambule et aux règles de la présente Charte.**

Seuls les administrateurs système du service de messagerie peuvent procéder, par obligation technique, à certains contrôles, mais ils sont tenus au secret professionnel et sont soumis à l'obligation de confidentialité. L'accès aux données enregistrées par les agents de l'université (dont les correspondances personnelles) ne peut être justifié que dans le cas d'un dysfonctionnement important.

## Article 7. Engagements de l'utilisateur

### Respect de la législation

L'utilisateur s'engage à respecter la législation en vigueur, évoquée à titre non exhaustif à l'article 1, et notamment :

- L'utilisateur s'engage à utiliser le service :
  - dans le respect des lois relatives à la propriété littéraire et artistique ;
  - dans le respect des lois relatives à l'informatique aux fichiers et aux libertés ;
  - dans le respect des règles relatives à la protection de la vie privée et notamment du droit à l'image d'autrui ;
  - en s'assurant de ne pas envoyer de messages à caractère raciste, pornographique, pédophile, injurieux ou diffamatoire ou de provocation ou apologie du terrorisme et de manière générale à ne pas diffuser d'informations présentant le caractère d'un délit.

    Sont ainsi également (mais pas exclusivement) interdits et pénalement sanctionnés :

- La contrefaçon de marque, les dessins ou modèles, bases de données, brevets ou autres droits de propriété intellectuelle ;
- La reproduction, représentation ou diffusion d'une œuvre de l'esprit (par exemple : musique, photographie, logiciel, œuvre audiovisuelle ou cinématographique …) ou d'une prestation de droits voisins (par exemple : interprétation d'une œuvre musicale par un artiste, phonogramme, vidéogramme, programme d'une entreprise de communication audiovisuelle) en violation des droits de l'auteur, du titulaire de droits voisins et/ou du titulaire des droits de propriété intellectuelle ou d'images de personnes sans autorisation.

- Lorsque l'utilisateur est amené à constituer des fichiers comportant des données à caractère personnel telles que définies par la loi du 6 janvier 1978 modifiée et de la législation en vigueur. Il veillera en particulier :
  - à respecter les procédures préalables en prenant l'attache du Délégué à la protection des données (DPO) d'UBE ;
    - à procéder à l'information préalable des personnes concernées quant à la destination du traitement de ces informations ;
    - à n'effectuer auprès de mineurs, aucune collecte d'informations concernant l'entourage familial, le mode de vie des parents, leur statut socioprofessionnel ;
    - à procéder à l'information préalable des personnes concernées quant au risque inhérent à internet que ces données soient utilisées dans des pays n'assurant pas un niveau de protection suffisant des données à caractère personnel.

## Préservation de l'intégrité du service

L'utilisateur est responsable de l'usage qu'il fait du service. Il assure notamment, à son niveau, la sécurité de ce service et s'engage à ne pas apporter volontairement de perturbation à son fonctionnement.

L'utilisateur s'engage à ne pas effectuer, de manière volontaire, des opérations pouvant nuire au fonctionnement de la messagerie. Il s'engage notamment à :

- limiter l'envoi de messages aux seuls destinataires réellement intéressés ou concernés, pour éviter la saturation du réseau et des serveurs et ne pas obliger les destinataires à lire des messages sans intérêt pour eux ;
- ne pas procéder à des envois massifs de courriers ;
- prévenir le risque de saturation des boîtes de messagerie et des serveurs en évitant de joindre à un même message des documents trop volumineux et en utilisant chaque fois que possible des outils de compression ;
- ne pas interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés ;
- ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, saturer les ressources ;
- ne pas introduire de virus et s'assurer de prendre les dispositions minimales de sécurité antivirus ;
- à informer immédiatement l'université de toute perte, de toute tentative de violation ou anomalie relative à une utilisation de ses codes d'accès personnels ou de la messagerie ;

- à utiliser autant que possible les adresses de messagerie fonctionnelles, ceci pour permettre la continuité de service[1] notamment en cas de départ ou d'absence prolongée de personnel.

## Fonctionnement normal du service

L'utilisateur s'engage à utiliser le service de manière la plus raisonnable possible. Il est recommandé de ne pas transmettre de messages en dehors des heures ouvrables.
Il est rappelé que l'envoi d'un message n'implique pas une réponse immédiate. Le destinataire dispose d'un délai raisonnable pour y répondre.

Il est recommandé afin de faciliter la circulation de l'information :

- d'indiquer, de manière explicite pour chaque message son objet, de n'aborder qu'un sujet à la fois et de ne le traiter que par un court message ;
- d'indiquer, pour les personnels, lors d'échanges non professionnels dans le sujet une mention particulière et explicite indiquant son caractère privé (ex. : personnel et confidentiel ou « privé »). Cette règle n'est pas applicable aux étudiants ;
- d'utiliser le marquage « Urgent » uniquement lorsqu'il est vraiment nécessaire afin d'éviter qu'il perde rapidement tout son sens ;
- d'insérer dans le texte du message envoyé son prénom, son nom (l'utilisateur) en qualité de signataire, complété avec la fonction , la composante (UFR, Laboratoire , Pôle, service), le lieu d'affectation (Bâtiment, numéro de bureau) , … en utilisant la fonction « Insertion de signature » ;
- d'indiquer dans le texte des messages envoyés la description brève des pièces jointes ;
- de privilégier le lien vers un document donné à son envoi en pièce jointe ;
- d'utiliser pour les pièces jointes des formats d'échanges standards (PDF …). Pour des raisons de sécurité, les Zip, les exécutables et les documents contenant des macros sont refusés ;
- de restreindre l'utilisation des caractères en majuscules. Un texte rédigé en majuscules est difficile à lire et peut être mal perçu par le correspondant.

La messagerie électronique peut être génératrice de souffrance. Une meilleure utilisation de l'outil permet d'améliorer la qualité de vie au travail. Des recommandations du CHSCT sont accessibles en annexe.

## Fonctionnement en cas d'absence ou de mutation de l'utilisateur

En cas d'absence de l'utilisateur, celui-ci s'engage à utiliser tant que possible le gestionnaire d'absence de l'outil de messagerie qui permet de renseigner le texte de la réponse automatiquement adressée à chaque expéditeur en précisant en particulier la période d'absence et les autres adresses où le message peut être envoyé en cas de nécessité.

Lors de la mutation d'un utilisateur, il convient d'éviter que sa boîte de messagerie continue à recevoir des messages au titre des fonctions qu'il quitte.

[1] Permettre aux demandes de suivre leur cours sans interruption et sans mettre en péril le fonctionnement de l'université et assurer ainsi un service normal.

En cas de départ définitif de l'université pour éviter que des courriers électroniques ne soient pas relevés, que des boîtes de messagerie demeurent inutilisées, que des messages personnels ou confidentiels soient lus par des agents qui n'en sont pas destinataires, l'utilisateur s'engage à suivre la procédure suivante :

- L'utilisateur envoie un message à ses correspondants habituels leur indiquant la date de son départ et leur signalant la boîte de messagerie auxquels ils devront envoyer leurs messages à partir de cette date au titre des fonctions qu'il quitte (adresse de messagerie de son successeur s'il est connu, boîte de l'intérimaire ou boîte fonctionnelle) ;
- Juste avant son départ, l'agent archive dans un fichier les messages qu'il doit transmettre à son successeur et remet ce fichier au secrétariat ou à son supérieur hiérarchique (ceci n'est pas applicable aux étudiants) ;
- L'utilisateur s'engage à transférer les messages qu'il reçoit durant la période où la messagerie reste active (article 10) après son départ et qui sont destinés à son ancien service (ceci n'est pas applicable aux étudiants).

Dans le cas de décès de l'utilisateur, ou s'il s'absente sans préavis et est injoignable, l'université se réserve le droit de supprimer tout message de réponse automatique ou redirection qui impacterait le bon fonctionnement des services. Un autre message de réponse automatique pourra être ajouté en tant que de besoin à la discrétion de l'université. Le service messagerie, sur demande écrite du président ou de ses délégataires pourra accéder à la boîte de messagerie afin de transmettre les messages nécessaires à la continuité de service. **C'est pourquoi il est recommandé d'utiliser les adresses de messagerie fonctionnelles plutôt que nominatives**.

## Décès ou radiation de l'utilisateur

Dans le cas du décès ou d'une radiation d'un utilisateur et notamment pour les besoins de la continuité de service, l'université pourra être amenée à supprimer tout message de réponse automatique qui aurait été rédigé et à mettre en place un nouveau message indiquant vers qui les expéditeurs doivent se tourner. Si une redirection des messages électroniques était en place, cette dernière pourrait également être supprimée.

De plus, le compte de messagerie est verrouillé ainsi que les accès aux services numériques à partir du compte de cette personne, 24 heures maximum après la saisie de l'information de décès ou de radiation dans la base de données des ressources humaines ou de la scolarité par les services habilités.

Les données de l'utilisateur sont cependant conservées afin de pouvoir être fournies en cas de réquisition judiciaire ou sur demande du Président de l'université pour assurer la continuité de service. Ce temps de conservation ne saurait excéder la durée normale de validité du compte sauf décision judiciaire contraire.

En cas de décès, la famille ne peut demander sans décision de justice la récupération des données.

## Modalités d'accès à une boîte de messagerie

Sur demande du président de l'université et en cas d'absence prolongée ou de décès d'un personnel, en invoquant la continuité de service pour justifier la transmission de certains messages, dans ce cas, l'accès à la messagerie est strictement encadré avec la présence de témoins (au moins 2 personnes) qui garantissent

la procédure. Les messages dont le sujet comporte « privé », « confidentiel » ou « personnel » ou dont l'objet est sans rapport avec la demande de continuité de service ne peuvent être accédés.

## Utilisation rationnelle et loyale du service

L'utilisateur s'engage à effectuer une utilisation rationnelle et loyale du service de messagerie, afin d'en éviter la saturation ou le détournement à des fins personnelles.

L'utilisateur est tenu de se déconnecter du service et de fermer son navigateur immédiatement après l'usage de sa messagerie électronique, en particulier si l'utilisation a lieu sur un équipement informatique ouvert au public. La responsabilité de l'université ne saurait être engagée en cas de non-respect de cette obligation.

L'utilisateur accepte que l'université puisse avoir connaissance des informations nécessaires à l'administration du service (données de volumétrie, incidents, nature du trafic engendré) et puisse prendre toutes mesures urgentes pour stopper toute perturbation occasionnée. L'université se réserve notamment la possibilité de stopper l'accès au service en cas d'utilisation excessive ou non conforme à son objectif tel que rappelé dans le préambule.

L'utilisateur s'engage à ne pas utiliser des listes d'adresses de messagerie, des listes de diffusion pour un objectif autre qu'administratif, pédagogique ou éducatif, tel que rappelé dans la présente Charte.

L'utilisateur s'interdit à l'occasion du service proposé par l'université de faire de la publicité sur des produits ou services du commerce.

L'utilisateur s'interdit de retransmettre un message électronique après l'avoir modifié, lui ou une de ses pièces jointes, sans mentionner explicitement les modifications effectuées. En cas de réutilisation d'une partie de son texte, cet usage doit être clair et ne pas modifier le sens initial du document.

L'utilisateur s'engage autant que faire se peut à disposer d'une protection antivirus sur les moyens informatiques qu'il utilise, et de désactiver des fonctions pouvant exposer le système aux virus. Si l'utilisateur est victime d'un virus dans une pièce jointe, il doit cesser tout envoi sur la messagerie et prévenir le responsable informatique de sa composante et ceux à qui les fichiers contaminés ont été envoyés voire ceux qui l'ont créé.

L'utilisateur en particulier s'engage à détruire les messages alarmants qui invitent à une rediffusion massive pour prévenir un risque de contamination par virus informatique. Sa rediffusion générale risque d'entraîner une saturation de la messagerie.

L'utilisateur s'engage également à se conformer aux dispositifs mis en place par l'université pour lutter contre les codes malveillants et les attaques par programmes informatiques.

## Particularités quant à l'utilisation de l'annuaire

En aucun cas, les données personnelles présentes dans l'annuaire sur lequel s'appuie le service ne peuvent être extraites, reproduites ou diffusées vers des tiers, sans l'autorisation expresse de la personne concernée, ni servir à l'envoi collectif de messages qui ne serait pas strictement justifié par un usage pédagogique, ou administratif, notamment dans le cas d'une démarche commerciale ou publicitaire, politique ou religieuse, contraire aux principes de neutralité de l'Éducation nationale et de l'Enseignement supérieur.

## Article 8. Listes de diffusion et adresses de messagerie électronique fonctionnelles

### Adresses ou listes fonctionnelles

Dans la limite de ses moyens techniques, l'université peut mettre à disposition des services qui le demandent, une ou plusieurs adresses de messagerie électronique fonctionnelles. Ces adresses ainsi créées permettent la distribution de messages électroniques à une ou plusieurs personnes et ainsi un travail collectif et la continuité de service en cas d'absence ou de départ de personnels.

Les normes de nommage de ces adresses de messagerie électronique fonctionnelles sont détaillées dans le document « Détails techniques relatifs à la messagerie électronique ».

La gestion de l'adresse (ajout/suppression d'abonnés) ainsi créée relève de la seule responsabilité du/des responsables de la demande. Les adresses de messagerie électronique fonctionnelles sont établies avec l'accord préalable des agents concernés.

Le responsable/gestionnaire de la liste devra être obligatoirement présent dans la base de données des personnels de l'université et disposer d'une adresse en « ube.fr ».

Il lui appartiendra de maintenir à jour la liste des destinataires. Pour cela, il est recommandé d'utiliser l'adresse électronique en « ube.fr » du destinataire si ce dernier est un personnel ou un étudiant de l'UBE. Il est également possible d'alimenter la liste des abonnés automatiquement (base de données, annuaire LDAP…).

Les adresses de messageries des abonnés autres qu'en « u-bourgogne.fr » seront acceptées uniquement à défaut d'une adresse en ube.fr.

Seul un responsable/gestionnaire de la liste pourra demander la modification de la liste des gestionnaires. Si le(s) responsable(s)/gestionnaire(s) ont quitté leur fonction et sont injoignables, sur décision du président ou du directeur général des services (DGS), il pourra être fixé un nouveau responsable/gestionnaire.

Les messages adressés aux adresses de messagerie électronique fonctionnelles font l'objet d'un archivage automatique. Cet archivage ne peut excéder 3 ans.

### Listes de diffusion institutionnelles

Les listes de diffusion institutionnelles relèvent de la responsabilité exclusive de l'université. Tous les personnels et étudiants sont inscrits à ces listes et n'ont pas la faculté de se désabonner.

L'université permet aux organisations syndicales l'usage ponctuel des listes de diffusion institutionnelles, pour des messages généraux d'information syndicale. Les règles d'usage sont précisées dans la Charte spécifique aux organisations syndicales.

Les listes de diffusion institutionnelles sont soumises à un circuit de modération sous la responsabilité du président et du directeur général des services. Toutefois, l'université ne pourra pas bloquer la diffusion d'un message, à l'exception des cas suivants :

- dépassement du nombre d'envois autorisés ;
- contenu contrevenant manifestement aux dispositions législatives relatives à la diffamation et aux injures, non conforme aux bonnes mœurs ou à la présente Charte.

## Article 9. Obligation particulière de confidentialité et discrétion

La sauvegarde du patrimoine et des intérêts de l'université passe par le respect, par l'utilisateur d'une obligation générale et permanente de confidentialité et de discrétion à l'égard des informations et documents électroniques disponibles sur le réseau interne, ce qui implique de :

- s'assurer du niveau de confidentialité des documents avant de les diffuser (bien respecter les directives présentes dans le mail s'il y en a) ;
- veiller à ce que des tiers non autorisés ne lisent pas de telles informations sur les écrans des ordinateurs ;
- ne pas rechercher ou ouvrir un message qui ne vous est pas adressé sans l'autorisation du destinataire ;
- en cas de réception d'un message par erreur, sans le lire, acheminer le message, vers le bon destinataire ou le rediriger vers son expéditeur ;
- vérifier qu'aucune erreur ne s'est glissée dans la sélection des destinataires.

L'utilisateur s'engage autant que faire se peut à ne pas communiquer son adresse de messagerie universitaire sur des serveurs web qui le demanderaient (en particulier lorsqu'il s'agit de remplir un formulaire), pour éviter de l'exposer à la réception de nombreux messages publicitaires.

## Article 10. Fonctionnement de la liste rouge

L'utilisateur peut décider de ne pas apparaitre dans l'annuaire public de l'université en décidant de figurer en liste rouge dont le fonctionnement est détaillé dans le document « Détails techniques relatifs à la messagerie électronique » ainsi que la manière d'y figurer.

## Article 11. Modalités de fermeture des accès

Sauf décision contraire du président ou du directeur général des services de l'université, le compte de messagerie reste accessible :

- Un an après le départ de l'université pour le personnel de l'université ;
- Jusqu'au 31 décembre de l'année suivant celle de sa dernière inscription administrative pour un étudiant ;

Par exception, la fermeture de la messagerie sera effective 24 heures maximum après la saisie de l'information de décès ou de radiation dans la base de données des ressources humaines ou de la scolarité par les services habilités :

- En cas de décès, de radiation, d'exclusion (uniquement pour les étudiants) ;
- Sur demande expresse de l'utilisateur auprès du président de l'université (en cas de départ de l'université).

L'université informera l'utilisateur par courrier électronique 45, 30 et 15 jours avant la clôture de son compte de messagerie. Les modalités de prolongation seront précisées dans ce courrier électronique.

L'université ne pourra être tenue pour responsable si ce message est placé dans le dossier spam de l'utilisateur et non lu.

Un compte de messagerie peut éventuellement être prolongé le temps d'effectuer les démarches nécessaires auprès du service des personnels sur demande du responsable administratif. Ce type de prolongation ne peut être que provisoire et défini dans le temps.

Les enseignants-chercheurs ayant fait valoir leurs droits et ayant fait une demande d'éméritat conservent leur compte de messagerie. Pour les chercheurs associés, il sera nécessaire de fournir aux services des personnels une attestation d'accueil signée par le directeur de laboratoire.

### En cas de divulgation des codes d'accès

S'il s'avère qu'un utilisateur a communiqué ses identifiants d'accès, le compte peut être verrouillé sans délai pour des raisons de sécurité. L'accès sera rétabli conformément aux modalités prévues à l'article 4.6.
Si un utilisateur communique ses codes d'accès notamment en répondant à un message électronique comme décrit à l'article 4 (mail de phishing) il expose l'université à une inscription sur liste noire chez les fournisseurs d'accès messagerie externes (Hotmail, orange, Gmail, …). Les messages venant de l'université sont rejetés par ces fournisseurs, conséquence grave et impactant toute l'université.
Le compte pourra être verrouillé sans délai pour des raisons de sécurité et en cas de récidive, des sanctions pourraient être appliquées.

### En cas d'inactivité

Uniquement en cas d'inactivité durant les deux mois suivants la création du compte de messagerie pour un personnel, le compte sera automatiquement verrouillé pour des raisons de sécurité. L'accès sera rétabli conformément aux modalités prévues à l'article 4.6.

**Il EST ENFIN PRECISE QUE LE NON-RESPECT DU CONTENU DE CETTE CHARTE PUISSE FAIRE L'OBJET DES LIMITATIONS ET SANCTIONS SUIVANTES**

## Article 12. Limitation des usages

En cas notamment de non-respect des règles définies dans la présente Charte et des modalités définies dans les guides d'utilisation, la « personne juridiquement responsable » pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre de l'utilisateur, limiter les usages par mesure conservatoire.

Par « personne juridiquement responsable », on entend : toute personne ayant la responsabilité de représenter l'université.
L'université se réserve le droit de supprimer sans préavis toute redirection susceptible de provoquer un dysfonctionnement des services ou pour des raisons de sécurité ou contraire à la présente Charte.

Tout abus à des fins extra-universitaires, dans l'utilisation des ressources mises à disposition de l'utilisateur, est passible de sanctions.

## Article 13. Sanctions

Le non-respect des règles établies ou rappelées par la Charte pourra donner lieu, indépendamment d'éventuelles sanctions judiciaires dont pénales, à la suspension de l'accès au service et à des sanctions de nature disciplinaire.

## Article 14. Dérogations

Toute demande de dérogation à la présente Charte devra être adressée au président de l'université pour validation à sa seule discrétion.

## Article 15. Entrée en vigueur de la Charte

La présente Charte a valeur de règlement intérieur pour ce qui concerne l'usage de la messagerie électronique et des services associés.

Président de l'Université Bourgogne Europe

Vincent Thomas

# CHARTE DE BON USAGE DES MOYENS NUMÉRIQUES DE L'UNIVERSITÉ BOURGOGNE EUROPE

*4 – Annexe juridique*

## S'applique à :

Tout personnel, étudiant et usager du système d'information de l'Université Bourgogne Europe (UBE)
Ci-dessous désignés par l'« utilisateur »

## Par :

L'Université Bourgogne Europe
Ci-dessous désignée par « l'Université » ou « UBE »

**Document présenté au CSA du 11/06/2025**

**Document voté par le conseil d'administration de l'Université Bourgogne Europe le 08/07/2025. Ce document vaut pour règlement intérieur.**

ENT : Environnement Numérique de Travail

**https://ent.ube.fr**

# SOMMAIRE

# 1. Les principaux textes réglementaires

**Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et Loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés**

- traitement automatisé ou non des données à caractère personnel ;
- Commission Nationale de l'Informatique et des Libertés (CNIL) ;
- obligations des responsables de traitements et droits des personnes ;
- délégué à la protection des données (DPO).

**Code général de la fonction publique portant obligations de secret professionnel, de réserve et de discrétion professionnelle,**

- devoir de moralité, de probité et de neutralité ;
- sanctions applicables aux personnels ingénieurs, administratifs, techniques, ouvriers et de service titulaires ;
- sanctions applicables aux agents administratifs contractuels.

**Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique**

- obligation des hébergeurs de contenus de lutter contre les infractions par la mise en place d'un dispositif de signalement (information des autorités publiques des activités illicites) ;
- obligation des hébergeurs de contenus de garantir la sécurité du stockage des données et de leur transmission.

**Code de l'éducation**

- sanctions applicables aux usagers de l'enseignement supérieur ;
- sanctions applicables aux enseignants-chercheurs et aux membres des corps des personnels enseignants de l'enseignement supérieur ;
- sanctions applicables aux autres enseignants.

**Code de la propriété intellectuelle**

- protection des œuvres de l'esprit ;
- protection des logiciels et des bases de données ;
- protection des marques.

**Code pénal**

- le secret professionnel (articles 226-13 et 226-14) ;
- le secret des correspondances (articles 226-15 et 432-9) ;
- la vie privée (articles 226-1 à 226-2-1) ;
- les droits de la personne résultant des fichiers ou des traitements informatiques (articles 226-16 à 226-24) ;
- les systèmes automatisés de données (articles 323-1 à 323-7).

## *Dispositions pénales loi du 29 juillet 1881 sur les crimes et délits commis par la voie de la presse ou par tout autre moyen de publication*

- Loi du 29 juillet 1881 sur la liberté de la presse : provocation aux crimes et délits articles 23 à 24 bis ; délits contre les personnes articles 32, 33 ;
- Code pénal : provocation ou apologie du terrorisme articles 421-2-5 à 421-5-1 Code pénal ; outrage sexiste ou sexuel.

### *a) Infractions prévues par le Nouveau Code pénal*

**Crimes et délits contre les personnes**

**Atteintes à la personnalité : (Respect de la vie privée art. 9 du Code civil)**

- atteintes à la vie privée (art. 226-1 al. 2 ; 226-2 al. 2, art.432-9 modifié par la loi n°2004-669 du 9 juillet 2004) ; atteintes à la représentation de la personne (art. 226-8) ;
- dénonciation calomnieuse (art. 226-10) ;
- atteinte au secret professionnel (art. 226-13) ;
- atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques (art. 226-16 à 226-24, issus de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

**Atteintes aux mineurs : (art. 227-23 ; 227-24 et 227-28).**

- Loi 2004- 575 du 21 juin 2004 (LCEN)

**Crimes et délits contre les biens**

- escroquerie (art. 313-1 et suite) ;
- atteintes aux systèmes de traitement automatisé de données (art. 323-1 à 323-7 modifiés par la loi n° 2004-575 du 21 juin 2004).

**Cryptologie Rançonlogiciel**

- Art. 132-79 (inséré par loi n° 2004-575 du 21 juin 2004 art. 37).

### *b) Infractions de presse (loi 29 juillet 1881, modifiée)*

- provocation aux crimes et délits (art.23 et 24) ;
- apologie des crimes contre l'humanité, apologie et provocation au terrorisme, provocation à la haine raciale, « négationnisme » contestation des crimes contre l'humanité (art. 24 et 24 bis) ;
- diffamation et injure (art. 30 à 33).

### *c) Infraction au Code de la propriété intellectuelle*

- contrefaçon d'une œuvre de l'esprit (y compris d'un logiciel) (art. 335-2 modifié par la loi n° 2004-204 du 9 mars 2004, art. 34 - et art. 335-3) ;

- contrefaçon d'un dessin ou d'un modèle (art. L521-4 modifiée par la loi n° 2004-204 du 9 mars 2004, art. 34) ;
- contrefaçon de marque (art. L716-9 - modifié par la loi n° 2004-204 du 9 mars 2004, art.34 -et suivants).

### *Code civil*

- Respect de la vie privée et droit à l'image (article 9).

Il est rappelé que cette liste n'est qu'indicative et que la législation est susceptible d'évolution.

## 2. Notions juridiques

### *La protection des données à caractère personnel*

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) - Loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés - Code pénal.

Toutes les informations relatives à des personnes physiques permettant de les identifier directement ou indirectement sont protégées par la loi qui encadre strictement leur collecte, leur traitement ou utilisation et leur conservation afin de garantir le droit des personnes.

Toute personne a un droit d'information et d'accès aux données à caractère personnel la concernant collectés ou non auprès d'elle, en vue de leur traitement (articles 12 à 15 RGPD).

En outre, sauf dispositions législatives contraires rendant obligatoire le traitement (article 23 RGPD), toute personne dispose sur ses données personnelles d'un droit de rectification, d'effacement (droit à l'oubli) et d'opposition notamment (articles 16 à 22 RGPD).

À l'UBE, ces droits s'exercent auprès du délégué à la protection des données (DPO) de l'établissement : dpo@ube.fr.
La CNIL est l'autorité administrative indépendante chargée par la loi de veiller au respect par le responsable du traitement du droit des personnes en matière de traitement des données nominatives à caractère personnel.

Ce traitement est réalisé automatiquement ou par un fichier manuel (fichier informatique ou fichier « papier »).

Le non-respect du droit des personnes en matière de collecte et de traitement des données personnelles est une infraction à la loi.

Exemple de sanction en cas d'infraction :
Article 226-16 du Code pénal : *« Le fait, y compris par négligence, de procéder ou faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq d'emprisonnement et de 300 000 euros d'amende. »*

### *La protection du droit des auteurs*

## Code de la propriété intellectuelle

L'auteur d'une œuvre de l'esprit jouit sur son œuvre « *d'un droit de propriété incorporel et exclusif opposable à tous* » (article L111-1 du Code de la propriété intellectuelle).

Les œuvres de l'esprit concernées par ce droit de propriété sont nombreuses et comprennent également les logiciels (article L112-2 du Code de la propriété intellectuelle).

Le principe à retenir, et à appliquer concernant l'utilisation de telles œuvres protégées est le suivant : une **autorisation expresse** des auteurs des œuvres (ou de leurs ayants droit) est obligatoire dès lors que cette utilisation excède le droit d'analyse et de courtes citations prévues par la règlementation (article L122-5 3°a) du Code*). Cette autorisation doit être écrite **dans une licence ou dans un contrat de cession de droits.**

**L'exception pédagogique** mentionnée par la règlementation (article L122-5 3° e) du Code*) est mise en œuvre sur la base d'un **contrat** entre le ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche, France université (ex- Conférence des Présidents d'Universités) et les représentants des titulaires de droits intéressés (Centre français du droit d'exploitation de la copie, SACEM, etc.). Ce contrat prévoit **une utilisation d'extraits de certaines œuvres protégées dans le cadre des activités d'enseignement, de recherche et de formation des enseignants et des chercheurs, ainsi que dans le cadre de l'élaboration et de la diffusion de sujets d'examens ou de concours organisés dans la prolongation de ces activités**. Il s'agit notamment des représentations en cours ou lors de conférences et de la mise en ligne sur le site intranet et espace numérique de travail (ERNEST). **Le public destinataire de ces œuvres doit être directement concerné par l'acte d'enseignement, de formation ou par l'activité de recherche**. Les œuvres utilisées conformément aux modalités prévues au contrat susmentionné font l'objet d'une contrepartie financière versée aux organismes gestionnaires des droits d'auteur qui se chargent de reverser aux auteurs ou éditeurs leur quote-part. Chaque établissement doit déclarer les utilisations d'œuvres réalisées annuellement notamment auprès du CFC pour le calcul de la rémunération forfaitaire des titulaires des droits.

Par « utilisation » de l'œuvre, on entend sa « reproduction » c'est-à-dire sa fixation sur un support matériel et/ou sa « représentation » c'est-à-dire sa communication à des tiers.
Toute utilisation d'œuvre doit être accompagnée de la **mention de ses références bibliographiques**.
Toute personne utilisant une œuvre de l'esprit en totalité ou partiellement sans autorisation écrite de l'auteur commet un délit, car elle se rend coupable de contrefaçon (articles L335-2 à L335-3 du Code).
Pour les logiciels, seule une copie de sauvegarde est tolérée, toute autre utilisation non consentie est un délit de contrefaçon (articles L122-6, L122-6-1 et L335-3 du Code).

Concernant les bases de données, les producteurs bénéficient en sus de la protection accordée aux auteurs d'œuvres de l'esprit, d'une protection du contenu de la base (article L341-1 du Code). À ce titre, l'utilisateur qui n'a pas obtenu les autorisations nécessaires auprès du producteur peut se rendre coupable de contrefaçon lorsqu'il d'une part, procède à des extractions du contenu de la base de données sur un autre support et d'autre part, réutilise en direction du public le contenu de la base (article 342-1 du Code).

Les marques (de fabrique, de commerce ou de service) peuvent également être protégées (article L711-1 du Code), si elles ont fait l'objet d'un enregistrement auprès de l'Institut national de propriété intellectuelle. Leur utilisation est soumise à l'autorisation de leur titulaire. À titre d'exemple, l'identité visuelle de l'établissement entre dans le champ de cette protection.

* Extraits du Code de la propriété intellectuelle - Article L122-5 - 3° a) et e) :

*« Lorsque l'œuvre a été divulguée, l'auteur ne peut interdire :*
*3° sous réserve que soient indiqués clairement le nom de l'auteur et la source :*

*a) Les analyses et courtes citations justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'œuvre à laquelle elles sont incorporées ;*

*e) La représentation ou la reproduction d'extraits d'œuvres, sous réserve des œuvres conçues à des fins pédagogiques et des partitions de musique, à des fins exclusives d'illustration dans le cadre de l'enseignement et de la recherche, y compris pour l'élaboration et la diffusion de sujets d'examens ou de concours organisés dans la prolongation des enseignements à l'exclusion de toute activité ludique ou récréative, dès lors que cette représentation ou cette reproduction est destinée, notamment au moyen d'un espace numérique de travail, à un public composé majoritairement d'élèves, d'étudiants, d'enseignants ou de chercheurs directement concernés par l'acte d'enseignement, de formation ou l'activité de recherche nécessitant cette représentation ou cette reproduction, qu'elle ne fait l'objet d'aucune publication ou diffusion à un tiers au public ainsi constitué, que l'utilisation de cette représentation ou cette reproduction ne donne lieu à aucune exploitation commerciale et qu'elle est compensée par une rémunération négociée sur une base forfaitaire sans préjudice de la cession du droit de reproduction par reprographie. »*

## La protection de la vie privée et le droit à l'image

**Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) et Loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés - Code civil - Code pénal**

Le respect de la vie privée et de l'image d'autrui sont des principes fondamentaux du droit (article 9 du Code civil).

Les atteintes à la vie privée et à l'image engagent la responsabilité civile et pénale des personnes qui en sont à l'origine.

(article 226-1 du Code pénal)

*« Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :*

*1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;*

*2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant*

*dans un lieu privé.*

*3° En captant, enregistrant ou transmettant, par quelque moyen que ce soit, la localisation en temps réel ou en différé d'une personne sans le consentement de celle-ci.*

*Lorsque les actes mentionnés aux 1° et 2° du présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.*

*Lorsque les actes mentionnés au présent article ont été accomplis sur la personne d'un mineur, le consentement doit émaner des titulaires de l'autorité parentale.*

*Lorsque les faits sont commis par le conjoint ou le concubin de la victime ou le partenaire lié à la victime par un pacte civil de solidarité, les peines sont portées à deux ans d'emprisonnement et à 60 000 euros d'amende*. »

(article 226-2 du Code pénal)

« *Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1.*

*Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.* »

## Le secret des correspondances privées

**Code pénal -Circulaire du 17 février 1988 (JO 9 mars)**

La notion de correspondance privée est définie par une circulaire du 17 février 1988 : il s'agit d'un « *(…) message exclusivement destiné à une (ou plusieurs) personne, physique ou morale, déterminée et individualisée.* »
En ce sens qu'elle relève de la vie privée de l'individu, la correspondance privée est protégée par le secret des correspondances.

Une communication électronique émise ou reçue a le caractère de correspondance privée.

La violation du secret de la correspondance est une atteinte à la vie privée (article 226-2 du Code pénal) sanctionnée pénalement (1 an à 3 ans d'emprisonnement et 45 000 euros d'amende - articles 226-15 alinéas 1 et 2 et 432-9 du Code pénal).

La consultation et le contrôle par l'employeur des messages électroniques identifiés comme « privés » par les agents sont possibles dans le cas :

- d'un dysfonctionnement important moyennant la mise en œuvre par l'employeur d'un dispositif d'information vis-à-vis des agents ;
- du risque ou de l'évènement particulier sans condition de mise en œuvre à la charge de l'employeur.

## L’atteinte aux systèmes automatisés de données

**Code pénal**

L’utilisateur d’un réseau informatique engage sa responsabilité pénale dans les cas suivants : (article 323-1 à 323-3 du Code pénal)

- s’il accède ou se maintient dans ce réseau frauduleusement (3 à 7 ans d’emprisonnement et 100 000 à 300 000 euros d’amende) et s’il en résulte la suppression / la modification de données ou l’altération du système (5 à 7 ans d’emprisonnement et 150 000 à 300 000 euros d’amende) ;
- s’il entrave ou fausse le fonctionnement du système (5 à 7 ans d’emprisonnement et 150 000 à 300 000 euros d’amende) ;
- s’il introduit, extrait, détient, reproduit, transmet, supprime ou modifie frauduleusement des données (5 à 7 ans d’emprisonnement et 150 000 à 300 000 euros d’amende).

Des peines complémentaires peuvent être encourues notamment (article L323-5 du Code pénal) :

- l'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille ;
- l'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.

## Les sanctions disciplinaires applicables aux utilisateurs du réseau informatique

**Code général de la fonction publique - Code de l’éducation - Décret n° 86-83 du 17 janvier 1986 relatif aux dispositions générales applicables aux agents contractuels de l'État**

L’établissement peut engager une procédure disciplinaire à l’encontre d’un utilisateur en infraction avec la charte informatique, cela quel que soit le statut de ce dernier, usager ou personnel (administratif titulaire ou contractuel, enseignant-chercheur, membres des corps des personnels enseignants de l’enseignement supérieur et autres enseignants), et indépendamment des poursuites pénales engagées à son encontre.

La procédure disciplinaire à l’encontre des usagers peut déboucher sur des sanctions allant de l’avertissement à l’exclusion de l’établissement, avec sursis ou non, ou l’exclusion de tout établissement d’enseignement supérieur public (article R811-11 du Code de l’éducation).

Les sanctions applicables aux enseignants-chercheurs et aux membres des corps des personnels enseignants de l’enseignement supérieur sont édictées par l’article 952-8 du Code de l’éducation qui prévoit 7 niveaux de sanctions, du blâme (1er niveau) à la révocation (7ème niveau). Deux sanctions intermédiaires étant l’abaissement d’échelon (3ème niveau) et l’interdiction d'exercer toutes fonctions d'enseignement ou de recherche ou certaines d'entre elles dans l'établissement ou dans tout établissement public d'enseignement supérieur pendant cinq ans au maximum, avec privation de la moitié ou de la totalité du traitement (5ème niveau).

Les sanctions applicables aux autres enseignants (article 952-9 du Code de l’éducation) sont classées en 4 niveaux : la sanction la moins élevée est le rappel à l’ordre, la plus élevée est l’interdiction d'exercer des fonctions d'enseignement ou de recherche dans tout établissement public d'enseignement supérieur soit pour une durée déterminée, soit définitivement. Les sanctions intermédiaires étant l'interruption de

fonctions dans l'établissement pour une durée maximum de deux ans (2ème niveau) et l'exclusion de l'établissement (3ème niveau).

Les personnels titulaires ingénieurs, administratifs, techniques, ouvriers et de service titulaires peuvent se voir infliger les sanctions prévues par le Code général de la fonction publique (article L533-1), celles-ci sont classées par groupes : l'exclusion temporaire de fonctions pour une durée maximale de trois jours (dernière sanction du 1er groupe) ; le déplacement d'office (dernière sanction du 2ème groupe) ; l'exclusion temporaire de fonctions pour une durée de seize jours à deux ans (dernière sanction du 3ème groupe) ; la révocation (dernière sanction du 4ème groupe).

Les sanctions applicables aux agents contractuels sont les suivantes (article 43-2 Décret n° 86-83 du 17 janvier 1986 relatif aux dispositions générales applicables aux agents contractuels de l'État)

1° L'avertissement ;

2° Le blâme ;

3° L'exclusion temporaire de fonctions pour une durée maximale de trois jours ;

3° bis L'exclusion temporaire de fonctions pour une durée de quatre jours à six mois pour les agents recrutés pour une durée déterminée et de quatre jours à un an pour les agents sous contrat à durée indéterminée ;

4° Le licenciement, sans préavis ni indemnité de licenciement.

**LA PRÉSENTE ANNEXE JURIDIQUE À SIMPLE VALEUR INFORMATIVE. ELLE FERA L'OBJET DE MISES À JOUR : IL APPARTIENT À L'UTILISATEUR DE PRENDRE CONNAISSANCE DE TOUTE NOUVELLE VERSION QUI SERA PUBLIÉE,**

Président de l'Université Bourgogne Europe

Vincent Thomas

# CHARTE DE DÉONTOLOGIE DES ADMINISTRATEURS DU SYSTÈME D'INFORMATION DE L'UNIVERSITÉ BOURGOGNE EUROPE

*5 – Déontologie des administrateurs*

## s'applique à :

Tout personnel, étudiant et usager du système d'information de l'Université Bourgogne Europe (UBE)
Ci-dessous désignés par l'« utilisateur »

## Par :

L'Université Bourgogne Europe
Ci-dessous désignée par « l'Université » ou « UBE »

**Charte présentée au CSA du 11/06/2025**

**Charte votée par le Conseil d'Administration (CA) de l'UBE le 08/07/2025. Cette charte vaut pour règlement intérieur.**

ENT : Environnement Numérique de Travail

**https://ent.ube.fr**

## Préambule

La fourniture des services liés aux technologies de l'information et de la communication s'inscrit dans la mission de service public de l'Enseignement Supérieur et Recherche (ESR).

Pour en assurer le fonctionnement, des agents employés spécifiquement (dénommés « administrateurs ») sont amenés à effectuer diverses opérations techniques pour fournir un service de qualité aux utilisateurs.

Ces opérations peuvent conduire les administrateurs à prendre connaissance d'informations de nature confidentielle, et doivent faire ceci en respectant les droits fondamentaux de l'utilisateur (protection des données personnelles, vie privée, secret des correspondances).

Aussi après avoir précisé le cadre technique de l'intervention des administrateurs, cette charte définira le cadre juridique de l'intervention des administrateurs.

SOMMAIRE

## Introduction

La présente charte constitue une annexe de la charte du numérique de l'Université Bourgogne Europe. Elle est librement consultable via l'environnement numérique de travail de l'Université Bourgogne Europe, dénommée UBE. Elle engage pleinement la responsabilité de l'agent en cas d'infraction, ou de complicité d'infraction, à la règlementation en vigueur et au règlement intérieur de l'université.

## Article 1. Rôle et responsabilité – définition des personnes

### *1.1 L'administrateur système*

Le terme « administrateur » désigne tout agent ayant pour mission d'assurer le bon fonctionnement ou la sécurité des ressources des systèmes d'information placées sous sa responsabilité dont, notamment, les serveurs, les équipements réseau, les équipements de sécurité, les applications, les bases de données ou les postes de travail.

La présente charte s'adresse à tout administrateur, quel que soit son statut : titulaire ou contractuel, ainsi que tout consultant ou prestataire.

Pour l'exécution de sa mission, l'administrateur dispose de droits d'accès privilégiés susceptibles de lui permettre l'accès à des informations, tels que des courriels, des fichiers, des données de connexion - confidentielles ou non - à caractère privé ou professionnel, dont il n'est ni le destinataire, ni l'auteur, ni le propriétaire.

Ces droits d'accès privilégiés lui permettent aussi d'entreprendre des actions potentiellement dangereuses pour les systèmes d'information tels que, par exemple, la modification ou le contournement de mécanismes de protection, la création ou la modification de comptes utilisateurs, la destruction ou la modification de fichiers.

L'administrateur est tenu au secret professionnel et soumis à l'obligation de discrétion professionnelle, il exerce ses missions dans le respect des prescriptions règlementaires régissant son statut, excluant de fait toute utilisation de ses droits d'accès privilégiés à des fins personnelles.

L'administrateur systèmes, réseaux et systèmes d'information est la personne, à laquelle a été confiée la responsabilité d'un système informatique, d'un réseau, d'équipements de téléphonie, de la maitrise d'œuvre d'application ou d'un traitement de données.

Les administrateurs sont donc autant de personnes différentes qui interviennent sur plusieurs éléments d'un système informatique (liste non exhaustive) :

- les  postes de travail individuels ;
- les bases de données, les systèmes d'exploitation du domaine ;
- le réseau, les applications (serveur/client) ;
- la téléphonie.

L'ensemble des éléments sur lesquels s'exerce cette responsabilité constitue le périmètre d'activité de l'administrateur.

### *1.2 Le Chargé de Sécurité des Systèmes d'Information (CSSI)*

Le Chargé de Sécurité du Système d'Information (CSSI) est la personne relais du Responsable de Sécurité du Système d'Information (RSSI) de l'établissement pour son entité. Suivant le périmètre de l'entité, un ou plusieurs CSSI peuvent être nommés.
De par son rôle dans la chaine de sécurité du système d'information, il pourra être amené à avoir accès à des informations des autres utilisateurs, informations parfois confidentielles.
Les règles de déontologie définies pour l'administrateur s'entendent également pour le CSSI.

### *1.3 Le Responsable de la Sécurité des Systèmes d'Information (RSSI)*

Le RSSI (responsable de la sécurité des systèmes d'information) est chargé de la définition et de la mise en œuvre de la politique de sécurité de l'établissement. Il possède en outre un rôle stratégique d'information, de conseil et d'alerte de la direction générale sur les risques en matière de sécurité informatique.
Les règles de déontologie définies pour l'administrateur s'entendent également pour le RSSI.

**L'ensemble de ces personnes sont désignées ci-dessous par « Administrateur »**

## Article 2. Droits de l'administrateur

**Dans le cadre de ses missions, un administrateur a le droit :**

- d'interrompre le fonctionnement de tout équipement, logiciel ou matériel, qui compromettrait la sécurité ou le bon fonctionnement d'un - ou d'un ensemble de – système(s) d'information ;
- d'utiliser des données de connexion et d'accéder à des informations privées professionnelles à des fins de diagnostic, de vérification, de métrologie, de statistiques ou en cas d'anomalie ou d'incident ;
- de prendre les mesures adéquates afin de prévenir tout risque de sécurité tel que virus, intrusion ou vol de données, destruction de données ou contournement de la politique de sécurité.

## Article 3. Devoirs de l'administrateur

**Dans le cadre de ses missions, un administrateur :**

- ne prend pas connaissance de données personnelles d'utilisateurs - sauf en cas de nécessité sur demande formelle AQSSI, DGS, FSD, sur demande formelle de l'utilisateur lui-même - et n'autorise quiconque à y accéder, sauf cas particulier prévus par la loi ;
- respecte les dispositions mentionnées dans la charte de bon usage des moyens numériques auxquelles sont soumis les administrateurs dans l'exercice de leurs missions, en particulier sur le

traitement des informations privées, sur la messagerie, sur le réseau Internet, sur la traçabilité, sur les mesures de contrôle et l'obligation d'information des utilisateurs ;

- respecte scrupuleusement la confidentialité des informations auxquelles il a accès et met en œuvre des mesures visant à assurer leur non-divulgation ;
- s'assure, avec le délégué à la protection des données (DPO) désigné, que la mise en œuvre du traitement respecte la règlementation sur la protection des données à caractère personnel ;
- informe le Responsable de la Sécurité des Systèmes d'Information (RSSI) de tout incident de sécurité ou toute faille de sécurité dont il pourrait avoir connaissance et respecte la chaine fonctionnelle de sécurité SI ;
- n'utilise ses droits d'accès privilégiés que ponctuellement et exclusivement pour les activités et les besoins directement liés à ses missions, et en aucun cas à des fins personnelles ;
- agis dans le sens d'une meilleure sécurité, dans l'intérêt de l'établissement et des utilisateurs ;
- Tout nouveau projet d'envergure mobilisant des moyens humains ou financiers importants, qu'il s'agisse de la mise en place d'une application, du lancement d'un développement ou tout projet qui utilise les outils, informations, bases de données qui sont hébergées au datacenter, doit être déclaré via une fiche projet accessible depuis l'ENT. Cette déclaration permet notamment de vérifier l'usage d'outils, de données ou de services hébergés au Datacenter, et d'éviter les redondances avec des projets existants ou en cours de déploiement.

## *3.1 Les missions*

### 3.1.1 Assurer un service de qualité aux utilisateurs

Les administrateurs ont la charge de la bonne qualité du service fourni aux utilisateurs dans la limite des moyens alloués. Ils ont aussi le devoir d'assurer l'intégrité, la disponibilité et la confidentialité des données échangées ou accessibles depuis le réseau informatique de l'université.
Aussi ils ont le droit :

- d'entreprendre toute démarche nécessaire au bon fonctionnement des ressources informatiques de l'université, et d'accéder à tout type d'information nécessaire à l'accomplissement de leur mission ;
- d'accéder à toute information utile à des fins de diagnostic et d'administration du système, en s'interdisant scrupuleusement de divulguer ces informations.

### 3.1.2 Transparence des opérations effectuées

Les administrateurs ont le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques.
De même ils s'engagent à informer l'utilisateur de toute opération inhabituelle tendant à accéder à ses données personnelles, directes ou indirectes, sur son poste informatique, et des motifs l'y autorisant conformément à l'exercice de ses missions (sauf au cas où la discrétion des opérations est imposée par les autorités judiciaires).

Tout matériel autre que les postes informatiques (PC, ordinateurs portables, etc.) destiné à être connecté au réseau filaire de l'UBE - tels que les objets connectés, robots, ajout d'équipement manageable et non manageable etc. - doit faire l'objet d'une demande préalable auprès de la DNUM avant tout achat. Cette demande permet de vérifier la compatibilité réseau, l'absence de risque de sécurité, ainsi que la disponibilité d'une prise réseau à l'endroit prévu pour l'installation.

### 3.1.3 Chaine d'alerte

Les administrateurs ont le devoir d'informer immédiatement leur responsable hiérarchique direct, le CSSI ou les CSSI de leur composante, laboratoire, service... ainsi que le RSSI de l'université (ou son suppléant) de toute tentative d'intrusion sur un système, de toute faille de sécurité détectée, ou de tout comportement d'utilisateur pouvant compromettre la sécurité du système informatique de l'université, dont il aurait eu connaissance pendant l'exercice de ses missions.

Le schéma de la chaine fonctionnelle est disponible via l'ENT ou l'intranet.

### 3.1.4 Sensibilisation des utilisateurs

Les administrateurs ont le devoir de sensibiliser les utilisateurs :

- rappeler les principes d'usage du réseau RENATER et les différentes chartes de l'UBE relatives aux systèmes d'information à tout utilisateur semblant les méconnaître ;
- informer les utilisateurs des consignes techniques de sécurité à mettre en œuvre afin de préserver le système informatique général et individuel ;
- sensibiliser aux risques juridiques encourus par l'université et eux-mêmes du fait de leur comportement (installation de logiciels sans licence, copies de sauvegarde sans autorisation, usage illégal ou non conforme des ressources informatiques) ;
- inciter les usagers à suivre les formations sur la Sécurité des systèmes d'Information présents au plan de formation UBE.

## 3.2 Les moyens

### 3.2.1 Les sauvegardes automatiques

Chaque application génère des fichiers de données informatisées qu'il convient de sauvegarder régulièrement pour assurer la continuité du service informatique en cas de perte ou d'altération de données. Ces données doivent être sauvegardées régulièrement de manière à assurer, dans la mesure du possible et selon les moyens disponibles, toute récupération de données.

### 3.2.2 La métrologie en temps réel

Un ensemble d'outils de supervision est actif pour l'ensemble du réseau de l'université pour en assurer un fonctionnement optimum. Ils permettent de faire de la métrologie (étude de la charge du réseau). Cette étude permet d'optimiser les ressources et de détecter les anomalies de fonctionnement, permettant ainsi à l'administrateur de procéder à une analyse plus fine en exploitant les « traces » d'opérations informatiques.

### 3.2.3 La traçabilité des opérations informatiques

Le bon fonctionnement et la sécurité du système informatique nécessitent l'enregistrement systématique et automatique d'un certain nombre d'informations caractérisant chaque opération informatique, appelées « traces ».
Ces traces sont toutes exploitables et peuvent conduire à reconstituer exactement un évènement informatique survenu, permettant ainsi à l'administrateur de réaliser la maintenance du service.

Ces traces ont deux objectifs exclusifs :

- → Assurer le bon fonctionnement des services et déterminer leurs améliorations possibles ;
- → Détecter toute anomalie de sécurité et être à même de mener les enquêtes correspondantes.

Elles sont exploitées sous forme de :

- statistiques non individuelles ;
- analyses par machine des opérations effectuées ;
- recherches manuelles précises sur un type de problème.

**Les administrateurs s'engagent à n'utiliser les traces que si un motif légitime les y oblige, conformément aux droits et devoirs que leur confèrent leurs missions.**

## Article 4. Cadre juridique de l'intervention

*« L'informatique ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »* (Article 1er de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers, et aux libertés).
Aucune exploitation, à des fins autres que celles liées à leurs missions, des informations dont les administrateurs ont connaissance pendant l'exercice de leurs missions, ne saurait être opérée, d'initiative ou sur ordre hiérarchique, qui aurait pour conséquence de violer les droits et libertés fondamentaux de l'utilisateur, tels que décrits ci-dessous.

Par conséquent, l'administrateur s'engage à respecter les droits fondamentaux des utilisateurs lors de l'exercice de ses missions, et plus particulièrement :

- le droit au respect de la vie privée ;
- le droit au secret des communications électroniques ;
- le droit au secret des correspondances.

**Par ailleurs, ils ont le devoir de désobéir à tout ordre qui aurait pour conséquence de leur faire commettre une infraction, que ce soit suite à la violation d'un droit fondamental de l'utilisateur tel que décrit ci-dessus, ou à la loi du 6 juillet 1978 modifiée en août 2004.**

Seules les autorités judiciaires, en tant que gardiennes des libertés individuelles, ont la faculté de déroger à ces principes en cas de nécessité liée à la recherche de preuves dans le cadre de l'instruction d'une affaire ou d'une enquête.

### *4.1 Respect de la loi relative à l'informatique, aux fichiers et aux libertés, RGPD*

La loi informatique et liberté pose des définitions ci-dessous énumérées, avant de poser les conditions de licéité d'un traitement de données personnelles, et les règles d'accès aux données personnelles de l'utilisateur sur son poste de travail.

### *4.2 Définitions / références juridiques*

Les principales dispositions légales en vigueur prévues par la législation française sont décrites dans l'annexe juridique associée à la charte de bon usage des moyens numériques de l'université (document principal).

Chaque administrateur devra connaître les définitions de :

- donnée à caractère personnel ;
- conditions de mise en œuvre d'un traitement automatisé de données à caractère personnel.

#### 4.2.1 Les obligations spécifiques de l'administrateur, responsable du fichier

Le responsable d'un traitement de données à caractère personnel est (sauf désignation expresse par les dispositions législatives ou règlementaires relatives à ce traitement) *la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens* ; c'est à lui qu'incombe :

- d'accomplir les formalités préalables à la mise en œuvre du traitement auprès du DPO ;
- d'informer l'utilisateur de l'identité du responsable du fichier, de celles des destinataires des données, des droits d'accès, de rectification et d'opposition dont il dispose ;
- assurer la sécurité des données contre toute altération, modification ou communication à des tiers non autorisés en prenant toute précaution utile ;
- recueillir le consentement préalable des personnes concernées.

#### 4.2.2 Les conditions de collecte des données et de traitement

Ces conditions s'appliquent à tout administrateur chargé de la mise en œuvre du traitement, lequel doit veiller à leur bonne application.

La collecte des données et leur traitement doivent être : « loyaux et licites ».

Pour des « *finalités déterminées, explicites et légitimes* » ;

### 4.2.3 Précautions particulières lors du traitement de données personnelles

Des précautions particulières s'imposent pour les administrateurs ayant connaissance de données à caractère personnel au cours de leur enregistrement, classement, transmission ou toute autre forme de traitement de données, afin d'éviter :

- toute divulgation, même par imprudence ou négligence ;
- de détourner ces informations de la finalité de leur traitement initial tel que défini par la disposition législative.

### 4.2.4 Accès aux données personnelles de l'utilisateur sur son poste de travail

L'administrateur s'engage à inviter l'utilisateur à classer ses données personnelles et professionnelles, chaque fois que cela est possible, avant chaque intervention sur son poste de travail, afin de respecter l'intimité de la vie privée de l'utilisateur et de délimiter plus facilement son cadre d'intervention comme défini ci-après.

**Il est recommandé à l'utilisateur de classer ses données dans un répertoire nommé « Privé ».**

#### Accès direct sur les postes (intervention sur site)

En tout état de cause, et lorsque l'intervention le nécessite, l'accès direct aux données enregistrées par les utilisateurs dans leur propre environnement informatique, qui sont parfois de nature personnelle, ne peut être justifié que dans les cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par d'autres moyens moins intrusifs, et si l'utilisateur a été informé (ce qui est implicite dès lors qu'il a autorisé l'administrateur à intervenir sur son poste de travail afin de résoudre un problème).

#### Accès indirect sur les postes (intervention à distance)

Toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant :

- De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;
- Des moyens dont elle dispose pour s'y opposer.

## *4.3 Obligation de confidentialité et secret professionnel*

Les administrateurs ayant la qualité de fonctionnaires sont soumis au secret professionnel de par leur statut général.
Les agents non titulaires, sans être astreints au secret professionnel, sont dans la nécessaire confidence concernant les informations dont ils pourraient avoir connaissance pendant l'exercice de leurs missions, et sont soumis, en ce qui concerne les données à caractère personnel dont ils pourraient avoir connaissance durant leur mission, à une obligation de non-divulgation.

L'administrateur a le devoir de transmettre tous les faits constitutifs de délits ou de crimes dont il aurait pu avoir connaissance durant l'exercice de sa mission en suivant la chaine fonctionnelle de sécurité des systèmes d'information.
Ces faits constitutifs d'infractions sont énumérés en annexe, sans être limitatifs aux seuls faits informatiques.

## 5. Engagements

L'administrateur s'engage à respecter en toute circonstance la législation en vigueur, ainsi que les règles de la PSSIE et de la présente charte ainsi que toutes les chartes régissant l'usage du système d'information.
Pour cela, il est accompagné à travers les dispositifs universitaires d'information et de formation.

**En cas de doute ou de question, l'administrateur du système d'information pourra demander conseil auprès :**

- **Du fonctionnaire Sécurité Défense**
- **Du service juridique**
- **Du DPO**
- **De la DNUM**

Président de l'Université Bourgogne Europe

Vincent Thomas

# CHARTE D'USAGE DU SYSTEME D'INFORMATION PAR LES ORGANISATIONS SYNDICALES DE L'UNIVERSITE BOURGOGNE EUROPE

*6 – Organisations syndicales*

## S'applique à :

Tout personnel, étudiant et usager du système d'information de l'Université Bourgogne Europe (UBE)
Ci-dessous désignés par l'« utilisateur »

## Par :

L'Université Bourgogne Europe
Ci-dessous désignée par « l'Université » ou « UBE »

**Présentée au CT du 9/05/2016**
**Votée par le conseil d'administration (CA) de l'institution le 31/05/2016**

**Charte présentée au CSA du 11/06/2025**

**Charte mise à jour et votée par le CA du 08/07/2025**
**Cette charte vaut règlement intérieur en ce qui concerne l'usage du système d'information par les organisations syndicales.**

ENT : Environnement Numérique de Travail

**https://ent.ube.fr**

## Préambule

Afin de faciliter la diffusion de l'information syndicale au sein de l'UBE, et dans le respect du code général de la fonction publique R213-33 relatif à l'exercice du droit syndical dans la fonction publique, il est mis à disposition des organisations syndicales du matériel informatique et des services numériques tels que les listes de diffusion, l'intranet et l'utilisation du réseau.

La présente charte définit les conditions d'utilisation du système d'information par les organisations syndicales dans le cadre de l'exercice de leur activité au sein de l'UBE.

La présente charte définit les conditions de mise à disposition par l'UBE des outils de communication électronique tels que la messagerie électronique interne ou l'intranet dans des conditions permettant de faciliter et de préserver tout à la fois :

- le droit à l'expression syndicale ;
- l'égalité de traitement des différents partenaires sociaux ;
- l'intégrité de l'outil de travail, propriété de l'UBE.

Cette charte complète la charte de bon usage des moyens numérique de l'UBE et la Charte d'utilisation de la messagerie électronique accessible notamment sur le site de l'Environnement Numérique de Travail de l'UBE.

# SOMMAIRE

# Article 1. Champ d'application

La présente charte précise les modalités d'utilisation des systèmes d'information par les organisations syndicales citées dans le préambule, sans que celles-ci puissent se substituer aux moyens d'expression existants et régis dans le respect du code général de la fonction publique R213-33 à l'exercice du droit syndical dans la fonction publique et à l'arrêté du 4 novembre 2014 relatif aux conditions générales d'utilisation par les organisations syndicales des technologies de l'information et la communication dans la fonction publique de l'État.

# Article 2. Mise à disposition de matériel informatique

L'équipement des locaux syndicaux en matériels et logiciels informatiques s'effectuera selon les mêmes modalités, notamment en termes de sécurité, que l'équipement professionnel des agents affectés dans le service au titre duquel les locaux syndicaux sont attribués.
Le matériel (ordinateur de bureau type bureautique) et les logiciels (système d'exploitation et suite bureautique) permettront la connexion gratuite au réseau et un accès à internet.

Le matériel informatique mis à disposition reste la propriété de l'université. La maintenance en sera assurée par les équipes informatiques à la demande des représentants syndicaux (sous forme de ticket dans le helpdesk).
Il sera renouvelé à la fin de son amortissement.

Pour imprimer, le raccordement à un photocopieur réseau sera effectué par les équipes informatiques. Pour assurer la confidentialité des impressions, elles pourront être envoyées au photocopieur en mode « privé », elles seront stockées et uniquement imprimées au moment où le « code privé » attribué au document sera saisi sur le photocopieur.

Un espace de stockage identique à celui mis à disposition des personnels administratifs de l'université pourra être mis à disposition pour effectuer une copie de données. Néanmoins, la sauvegarde des données restera sous la responsabilité de l'organisation syndicale. L'université ne pourra pas être tenue pour responsable en cas de perte de données.

# Article 3. Messagerie électronique

## *3.1 Attribution d'adresses électroniques syndicales*

L'UBE s'engage à attribuer à l'organisation syndicale une adresse électronique clairement identifiable (adresse fonctionnelle) lui permettant d'émettre et de recevoir des messages.

Pour cela :

- Un formulaire de demande de création en ligne de liste fonctionnelle devra être renseigné ;
- La dénomination de cette adresse syndicale devra faire apparaître explicitement le nom[1] de l'organisation.

[1] Pour exemple <nom de l'organisation syndicale>@ ube.fr ou <nom de l'organisation syndicale>.<complément contextuel>@ube.fr

L’adresse électronique de l'organisation syndicale ne se substitue pas à celle de l'agent représentant de l'organisation ; ainsi celui-ci devra utiliser l’adresse fonctionnelle pour toute communication d’expression syndicale.

L'accès à cette adresse est autorisé depuis tout poste de travail.

Les adresses électroniques bénéficieront d’auto modération pour des raisons de sécurité.

## *3.2 Nature des messages électroniques*

Les adresses électroniques syndicales ont vocation à être utilisées pour les activités syndicales, notamment pour la correspondance avec les adhérents, sans autre limitation que celles définies dans la charte de bon usage des moyens numériques de l’UBE et la charte d’utilisation de la messagerie électronique.

L'adresse électronique de l'organisation syndicale peut servir aux échanges avec tout personnel de l’université de façon individualisée (à l’initiative de l’agent) ou par le biais de listes de diffusion préétablies (Cf. section 3.3).

Pour la diffusion d'informations syndicales à caractère général, l’organisation syndicale privilégie la publication sur l'espace intranet qui lui est réservé et non l’envoi de masse sur les adresses de messagerie des personnels de courriels avec une ou des pièces attachées. Les conditions d'utilisation de l'intranet sont précisées à l’article 4.

Dans le cas de communication individualisée, chaque personnel reste libre de demander par retour de courriel à ne pas être destinataire de ce type de message et l’organisation syndicale s’engage à ne plus contacter le personnel de manière individualisée.

## *3.3 Listes de diffusion*

Sur demande du syndicat, des listes de diffusion par type de population alimentées automatiquement et contenant initialement tous les personnels de l’établissement titulaires d’une adresse électronique en « @ube.fr » pourront être créées (cela comprend également les doctorants et personnels hébergés des laboratoires). Pour cela, un formulaire de création de liste de diffusion syndicale devra être renseigné.

Ces listes de diffusion seront utilisées par l’organisation syndicale afin de permettre la diffusion d’informations syndicales. Dans une optique de sobriété énergétique, il est recommandé de privilégier l’envoi de courriels sans pièce jointe. La taille d’un message diffusé sur la liste est limitée actuellement à 5 Mo (pièces jointes comprises). Cette limite sera toujours précisée dans la demande de création de liste de diffusion syndicale. Cette taille pourra évoluer uniquement à la hausse en fonctions des évolutions technologiques.

Chaque personnel reste libre, conformément à la réglementation, de demander à ne plus être destinataire des messages d’information de l’organisation. À cet effet, un pied de page sera ajouté automatiquement à chaque message et renseignera le destinataire sur la procédure à suivre afin de ne plus recevoir les messages de cette liste s’il le désire.

La création de la liste de diffusion est de la compétence de la direction du numérique. Le syndicat ne peut pas consulter ou altérer la liste des abonnés.

Seuls les expéditeurs définis par l'organisation syndicale dans « demande d'accès aux listes de diffusion syndicale … » en annexe de cette charte sont autorisés à émettre des messages à destination de ces listes de diffusion. Les listes sont sous la seule responsabilité de l'organisation syndicale ou de son représentant.

### *3.4 Confidentialité des échanges*

L'UBE s'engage à prendre les mesures appropriées en vue d'assurer la confidentialité :

- des messages électroniques en provenance ou à destination d'adresses électroniques fonctionnelles syndicales (contenu, auteurs et destinataires) ;
- de la liste des adresses contenues dans la liste de diffusion élaborée par l'organisation syndicale.

Tout auteur d'actes d'interception, d'usurpation, d'altération de correspondances s'expose à des sanctions pénales et/ou disciplinaires.

L'UBE dégage toute responsabilité sur des faits qui seraient commis par un tiers.

## Article 4. Accès à l'Intranet

### *4.1 Droits d'usage*

L'UBE s'engage à mettre à disposition de l'organisation syndicale un espace de publication sur son intranet institutionnel. Un lien en page d'accueil permettra de renvoyer vers les pages d'expression syndicale.

L'ouverture de cet espace dédié s'effectue sur demande explicite du représentant officiel de l'organisation syndicale. Cet espace permet la mise à disposition de tout personnel des informations d'expression syndicale sous la responsabilité éditoriale et technique de l'organisation syndicale.

Lorsqu'un envoi de masse sur les adresses de messagerie est accompagné d'une ou plusieurs pièces jointes qui risquent de dépasser en taille le quota alloué, l'organisation syndicale devra procéder de la manière suivante :

- Stocker les fichiers (pièces jointes) sur les pages intranet mises à leur disposition ;
- Envoyer le courriel en masse pour informer les personnes avec un ou plusieurs liens hypertextes pointant sur le ou les fichiers stockés sur l'intranet.

Cette solution devra être privilégiée pour des raisons de sécurité, quelle que soit la taille des pièces jointes.

### *4.2 Gestion de l'espace dédié et de ses contenus*

L'organisation syndicale s'engage à limiter sur son espace dédié la publication aux seules informations d'expression syndicale à caractère général avec la possibilité de renvois vers d'autres sites syndicaux sur l'intranet ou l'internet.

### *4.3 Formation*

L'université prendra à sa charge la formation des membres du syndicat à l'utilisation des outils informatiques mis à leur disposition.
En complément, une formation peut être mise en place pour permettre aux représentants de l'organisation syndicale qui le souhaitent d'acquérir les compétences nécessaires à la mise en ligne des pages sur l'espace

intranet réservé, de l'utilisation des listes de diffusions ainsi qu'une sensibilisation à la sécurité du système d'information.

## Article 5. Accès au réseau

*L'UBE accorde au syndicat, l'accès au réseau de transmission de données universitaire (depuis le local qui est mis à leur disposition).* Il est rappelé que tout poste raccordé au réseau doit être déclaré au préalable auprès de la direction du numérique et, avant de procéder à son achat, respecter les règles de sécurité notamment la création d'une session par utilisateur du poste de travail.

## Article 6. Engagements de l'UBE

L'UBE s'engage à :

- mettre à disposition de l'organisation syndicale des listes de diffusion par type de population ;
- tenir cette liste à jour, compte tenu des arrivées et des départs, de manière automatique ;
- respecter les droits et possibilités d'expression de l'organisation syndicale signataire ;
- ne pas modérer les messages envoyés par l'organisation syndicale signataire, sauf dans le cas de non-respect de l'article 7.

## Article 7. Engagements de l'organisation syndicale

L'organisation syndicale signataire de la présente charte s'engage à :

- respecter les règles de la charte de bon usage des moyens numériques à l'UBE et de la charte de messagerie ;
- respecter les règles de confidentialité permettant de respecter les libertés individuelles et collectives ;
- respecter les règles de déontologie élémentaires liées au respect des personnes et des institutions ;
- respecter la limite d'une centaine de messages par an (moyenne annuelle) à l'attention des abonnés de la liste de diffusion syndicale ;
- respecter et faire respecter dans sa globalité la charte dès sa date de mise en œuvre.

## Article 8. Responsabilité du contenu

Les communications syndicales restent sous la responsabilité éditoriale et technique de l'organisation. La diffusion d'information à caractère injurieux, raciste, pornographique ou diffamatoire est strictement prohibée, et pourra faire l'objet de mesures disciplinaires et/ou judiciaires.

La mise en ligne des informations sur l'espace dédié s'effectue sous la responsabilité technique et éditoriale de l'organisation syndicale : une mention sur la page d'accueil de l'espace dédié à l'organisation syndicale le précise.
Le contenu de ces intranets ne saurait engager la responsabilité civile ou pénale de l'UBE.
L'organisation syndicale doit :

- respecter strictement les lois et règlements relatifs au droit d'expression syndicale, au droit de la presse, à l'abus de droit et au droit d'auteur ;
- respecter le droit de la fonction publique et notamment le droit de réserve.

Le règlement des usages des systèmes d'information de l'UBE doit être respecté.

Les mesures de sécurité mises en place par l'UBE et l'ensemble des chartes et notamment la charte de bon usage des moyens numériques de l'UBE et la Charte d'utilisation de la messagerie électronique s'appliquent dans ce cadre.

La nature et le contenu des pages d'information pourront faire l'objet d'éventuelles contestations devant les juridictions compétentes.

Les organisations syndicales gèrent les listes de diffusion conformément à la loi du 6 janvier 1978 relatives à l'informatique, aux fichiers et aux libertés. Dans ce cadre tout traitement sera sous l'unique responsabilité de l'organisation syndicale pour l'ensemble des obligations de la loi (demandes auprès de la CNIL, droits d'accès ...).

Les organisations syndicales doivent s'assurer que les documents syndicaux diffusés ou publiés respectent les éventuels droits de propriété intellectuelle des tiers, y compris ceux de l'Université Bourgogne Europe (logo par exemple). L'établissement ne pourra être tenu responsable en cas de manquement à cette obligation.

## Article 9. Mesures conservatoires

En cas d'inobservation des termes de la présente charte ou des autres chartes en vigueur à l'UBE, des lois et des règlements en vigueur, l'université se réserve le droit de suspendre, à titre temporaire, tout accès aux services tels que définis aux sections 3.1 (attribution des adresses électroniques), 3.3 (Listes de diffusion) et 4 (Accès à l'intranet).

Le non-respect des modalités d'utilisation peut conduire :

- Pour la messagerie : à la fermeture des adresses électroniques de l'organisation syndicale, à la suppression de la possibilité d'utiliser les listes de diffusion ;
- Pour l'intranet : à la demande de modifications d'éléments publiés ou à la suppression des textes non conformes.

## Article 10. Entrée en vigueur de la charte

Le présent document annule et remplace tous les autres documents ou chartes relatifs à l'utilisation des systèmes d'information par les organisations syndicales.

Il peut être mis fin à cette charte de plein droit par l'UBE, notamment en cas de manquement aux règles d'usage précitées.

Président de l'Université Bourgogne Europe

Vincent Thomas