Charte informatique des étudiants

- Télécharger la Charte informatique au format PDF

Préambule

À l'heure où les systèmes d'information, de communication et les services numériques sont de plus en plus interconnectés, la transformation numérique est à la fois marqueur de progrès et catalyseur de risques. Si les bénéfices ne sont plus à prouver, la fiabilité des services numériques sera garantie à la seule condition que les systèmes soient sécurisés et que les données soient protégées.

Du fait de ses activités et de sa mission de service public, l'université Bordeaux Montaigne doit garantir un niveau de sécurité adapté aux informations qu'elle est amenée à traiter.

Prenant en compte les préconisations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et de la Commission nationale de l'informatique et des libertés (CNIL), ce texte s'inscrit dans le cadre législatif et réglementaire en vigueur relatif à la protection des données à caractère personnel, à l'utilisation des logiciels, aux droits et obligations des étudiants utilisateurs des services numériques. Il s'inscrit dans les politiques de sécurité du système d'Information de l'université Bordeaux Montaigne.

Glossaire, sigles et abréviations

Terme	Définition
Cnil	Commission nationale informatique et libertés.
DPD	Délégué à la protection des données
DPO	Data Protection Officer : délégué à la protection des données
RSSI	Responsable sécurité des systèmes d'information
SSI	sécurité des systèmes d'information

Article 1. Portée et opposabilité

La présente charte et les modifications ultérieures qui pourraient intervenir sont applicables dès son approbation par le conseil d'administration de l'université. En conséquence, elle est opposable à l'Utilisateur des services numériques et il est supposé en avoir pris connaissance.

Aucune clause dudit document n'a pour but de déroger aux statuts et règlement intérieur de l'université, ou aux droits des représentants du personnel et des sections syndicales de l'université, ni d'apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché conformément à la législation en vigueur.

Article 2. Champ d'application

L'objet de la présente charte est d'informer les étudiants utilisateurs des services numériques de l'université Bordeaux Montaigne de leurs droits et obligations. Elle a été élaborée dans le souci de concilier les intérêts de l'université Bordeaux Montaigne avec ceux des étudiants.

Elle décrit ainsi l'ensemble des règles générales et spécifiques que chaque étudiant doit respecter dans l'utilisation des ressources et services numériques de l'université Bordeaux Montaigne, de manière à éviter de porter atteinte à la sécurité de l'université Bordeaux Montaigne, à la sécurité publique ou à la sécurité des usagers.

Chaque étudiant doit être conscient de l'impact de son usage quotidien ou occasionnel sur la sécurité des services numérique, et s'engage à accepter ce règlement dans tous ses éléments et à le respecter dans tous ses termes.

Dans le cas d'une UMR, celle-ci peut prévoir des restrictions d'accès spécifiques à son organisation. Les Utilisateurs de ces unités sont notamment également soumis au respect, quand elles existent, des politiques de sécurité du système d'information de l'unité édictées par les tutelles correspondantes (universités, CNRS, INSERM, INRIA, etc.).

Article 3. Definitions

Les définitions suivantes s'appliquent dans la suite du document :

* **Université** : l'Université Bordeaux Montaigne.
* **Administrateur** : toute personne (ou groupe de personnes) chargée(s) de l'exploitation, de la maintenance et de la supervision d'un service numérique, ou d'une partie de ce dernier.
* **Services numériques** : ensemble de processus et de ressources mis à disposition par l'université, permettant d'acquérir, de générer, de traiter, de stocker, de détruire, de diffuser, de transmettre ou d'accéder à des informations électroniques.
* **Ressources numériques** : ensemble de moyens informatiques et de télécommunications, matériels ou logiciels, que l'université Bordeaux Montaigne met à disposition des Utilisateurs afin que ceux-ci puissent accomplir leurs tâches professionnelles. Ainsi, les micro-ordinateurs fixes ou portables, les moyens de communication (accès à l'Internet, réseaux de transmission voix ou données, téléphones

fixes ou portables, télécopieurs, service de visio-conférence, etc.), les équipements de stockage de données (disques durs externes, clés USB, supports optiques tel que le DVD etc.), les données contenues sur les équipements précédemment cités, les applications informatiques et autres logiciels font partie des ressources du système d'information de l'université Bordeaux Montaigne.

Article 4. Principes directeurs

Il appartient à chacun d'adopter un comportement professionnel et responsable lors de l'utilisation des services et des ressources numériques afin de ne pas perturber ou entraver leur bon fonctionnement, ni entrainer un détournement des activités à des fins non-professionnelles ou illégales.

4.1 Usage « professionnel » des services et des ressources numériques

L'ensemble des services et des ressources numériques est mis à disposition des étudiants pour un usage « professionnel », c'est-à-dire toute activité scolaire et périscolaire en lien avec l'université.

4.2 Usage « privé » des services et des ressources numériques

L'utilisation à des fins privées des services et ressources numériques est tolérée dans la limite raisonnable liée aux nécessités de la vie courante et familiale.

Cet usage raisonnable à titre extra-professionnel doit être loyal, mesuré et ne peut en cas se faire au détriment des tâches ou missions « professionnelles » incombant à l'étudiant. Il ne doit en aucun cas nuire au bon fonctionnement de l'ensemble des ressources numériques de l'université ou altérer son image.

4.3 Confidentialité des informations et des données

La protection du patrimoine numérique de l'université et ses intérêts supposent le respect par chaque étudiant d'une obligation de confidentialité à l'égard des informations dont il a connaissance dans l'exercice de ses activités.

Dans ce cadre, l'étudiant se doit de respecter certaines règles :

* l'étudiant est soumis à une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède ;
* l'étudiant ne doit pas tenter d'accéder ou prendre connaissance d'un message électronique qui serait adressé à un autre destinataire sans l'autorisation formelle de ce dernier ;
* en aucun cas, l'étudiant ne doit révéler à quiconque ses moyens d'accès aux services et aux ressources numériques (ses mots de passe, code PIN ou tout autre secret d'authentification) qui sont strictement personnels et incessibles.

4.4 Dispositions législatives et réglementaires

Tout étudiant doit respecter les dispositions législatives et réglementaires relatives à l'utilisation des technologies de l'information et de la communication. Celles-ci prévoient en particulier les mesures interdisant :

* l'atteinte à la vie privée (i.e. opinions politiques, religieuses, philosophiques, aux origines ethniques, à la vie sexuelle ou à la santé des personnes) ;
* les actes de violence écrite ou verbale ou contraire aux règles éthiques ou aux bonnes mœurs, notamment :
* la diffamation et l'injure,
* le révisionnisme et l'apologie des crimes, notamment meurtre, viol, crime de guerre et crime contre l'humanité,
* l'incitation aux crimes et délits (i.e. l'incitation au suicide, à la haine ou à la violence),
* l'atteinte aux mineurs (i.e. exposition à des messages à caractère violent, pornographique ou pédopornographique,
* l'incitation à la consommation de substances interdites ;
* la fraude informatique, incluant des actes tels que :
* l'accès ou le maintien frauduleux dans un système de traitement automatisé de données,
* la falsification, la modification, la suppression et l'introduction d'information avec l'intention de nuire ;
* la violation du secret professionnel, des affaires, des enquêtes et de l'instruction ;
* la violation de la propriété intellectuelle et du droit à l'image ;
* le non-respect de la réglementation relative à la protection des données à caractère personnel.

Article 5. Règles d'utilisation générales

5.1 Accès aux ressources et services numériques

Par principe, chaque étudiant n'a accès qu'aux services ou ressources numériques qui lui sont nécessaires dans le cadre de son activité. Les droits d'accès à tout ou partie des services ou ressources numériques reposent sur une identification/authentification de chaque étudiant qui ne doit en aucun cas chercher à accéder par des moyens détournés ou fortuits à des informations et/ou ressources pour lesquelles il n'est pas habilité.

Les moyens d'authentification (i.e. mots de passe, code PIN ou tout autre moyen d'authentification) aux services ou ressources numériques sont strictement personnels et incessibles. Le respect de ces principes est de la responsabilité des étudiants et des autres utilisateurs.

5.2 Données personnelles de l'étudiant

La conservation de données, documents, fichiers et messages électroniques à titre privé est tolérée aux conditions strictes que l'usage soit raisonnable, que cela ne nuise pas

au bon fonctionnement et à la sécurité des services numériques, et que ces derniers ne contreviennent pas aux lois et à la réglementation en vigueur (i.e. données à caractère pédopornographique, pornographique, injurieux, diffamatoire, raciste, violent, faisant l'apologie du terrorisme ou d'actes illicites, etc.).

Ces données sont considérées comme privées dans la mesure où le marquage spécifique « PRIVE » ou « privé » est employé pour les identifier explicitement (dans le nom des fichiers, le nom du répertoire de stockage ou dans l'objet du message électronique).

Tout document, contenu ou message électronique qui ne comporterait pas ce marquage, sera alors considéré comme professionnel. L'université pourra y avoir accès même en l'absence de l'étudiant.

En application de ces principes, le répertoire « Mes documents » de chaque utilisateur est réputé professionnel. Cependant, l'espace de documents nommé « Privé » sur le bureau virtuel est considéré comme un espace privé.

L'étudiant ne doit, en aucun cas transformer et/ou qualifier des données, documents, fichiers ou messages de nature professionnelle en données, documents, fichiers ou messages privés.

À la fin de l'année universitaire, le compte de l'étudiant reste actif jusqu'au mois de décembre suivant s'il ne se réinscrit pas (en cas de réinscription, le compte est conservé pour une année).

L'étudiant doit donc faire le nécessaire avant son départ pour sauvegarder toutes ses données dont il pourrait avoir besoin ultérieurement.

5.3 Protection du patrimoine numérique

L'université sauvegarde de manière automatique tout ou partie des données (répertoires, messages électroniques, etc.) présentes sur ses services et ressources numériques de manière à en garantir la disponibilité en cas d'incident. Les sauvegardes sont faites sans distinction des répertoires (privés ou non) de l'étudiant.

L'étudiant est toutefois responsable de la sauvegarde et de la récupération de ses données, fichiers, documents et messages électroniques marqués « PRIVE » ou « privé ».

5.4 Protection des informations contenues dans les équipements informatiques et supports amovibles

Le matériel informatique et de télécommunication que l'université fournit est placé sous la responsabilité de l'étudiant, en tous lieux et en toute circonstance.

A ce titre, l'étudiant doit utiliser les moyens de protection mis à sa disposition (câble antivol, armoire sécurisée, etc.) et appliquer les consignes de sécurité (verrouillage de l'ordinateur) afin de se prémunir contre le vol d'information. Lors de l'utilisation d'équipements nomades ou mobiles (notamment lors de voyages ou déplacements), les risques de compromission

potentielle de l'information sont plus élevés. L'étudiant doit donc faire preuve d'une vigilance accrue pour en assurer la surveillance. En cas de perte ou de vol, il doit le signaler dans les plus brefs délais à son responsable administratif et au service informatique de proximité (qui informera le RSSI), qui lui indiquera la procédure à suivre.

Enfin, l'étudiant doit faire preuve d'une attention particulière lors de l'emploi des supports amovibles de stockage de masse (tels clés USB, disques durs externes, etc.) dont l'usage est fortement déconseillé. Les supports de stockage fournis par l'université ne doivent pas être prêtés ni connectés à des ordinateurs autres que ceux fournis par l'université.

5.5 Protection du matériel

Chaque étudiant contribue à la protection des informations conservées sur les équipements mis à sa disposition. Dans cette perspective, il se doit notamment de respecter toutes les mesures élémentaires visant à ne pas introduire et diffuser de programmes malveillants, à ne pas entraver le bon fonctionnement des contrôles de sécurité ou y porter atteinte de manière volontaire. L'étudiant s'assure de :

* ne pas mettre en œuvre d'outils susceptibles de contourner ou d'affaiblir la sécurité des services numériques de l'université ;
* ne pas stocker, transférer ou transmettre des informations professionnelles, qu'elle qu'en soit leur nature, via des dispositifs non autorisés par l'université ;
* ne pas exploiter les éventuelles failles de sécurité, en faire la publicité ou les divulguer à des tiers ;
* ne pas altérer la configuration de ses équipements notamment en ce qui concerne le paramétrage des dispositifs de sécurité tels que l'antivirus, le pare-feu, le verrouillage de l'écran de veille, etc.

Seul le matériel mis à disposition par les services informatiques internes peut être connectés aux infrastructures informatiques et de télécommunication de l'université. En particulier, le matériel personnel des étudiants ne peut être connecté qu'au réseau Wifi ou au réseau « invités ».

Enfin, l'étudiant doit restituer tout matériel informatique et de télécommunication confié par les services Informatiques (poste de travail portable, etc.) lorsqu'il quitte l'université.

5.6 Services Internet

L'utilisation d'Internet n'est autorisée que dans le cadre de l'usage administratif ou pédagogique. Toutefois, un usage raisonnable des services de l'Internet est toléré dans le cadre des nécessités de la vie courante et familiale, à condition que son utilisation n'affecte pas les performances des services numériques de l'université ou ne perturbe pas le travail de l'étudiant.

L'université se réserve le droit de bloquer ou de limiter l'accès, au travers de dispositifs de filtrage ou de sécurité, à tout contenu présentant un risque légal, d'image ou d'atteinte à la

sécurité de l’université ou des étudiants tels qu’un site malveillant, pornographique, etc. ou incompatibles avec l’activité administrative ou pédagogique.

Les contenus en ligne susceptibles d’entrainer une consommation importante des ressources Internet peuvent également être réglementés par l’université.

Par ailleurs, l’étudiant utilisateur des services de l’Internet s’engage à ne pas utiliser les ressources de l’université pour tenir des propos (oraux ou écrits) qui seraient considérés comme illicites ou contraires à l’ordre public, à ne pas porter atteinte à l’intégrité d’un autre utilisateur ou à sa sensibilité notamment par des messages, textes ou images provocants et à ne pas émettre d’opinion personnelle étrangère à son activité professionnelle ou susceptible de porter préjudice à l’université. Les étudiants sont fortement encouragés à respecter les règles de politesse d’usage sur l’Internet.

5.7 Messagerie électronique

L’étudiant se voit attribuer une adresse électronique institutionnelle lors de son inscription. Cette adresse électronique est mise à disposition pour un usage en lien avec ses études.

Cependant, un usage raisonnable et ponctuel de la messagerie électronique dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages institutionnels. Tous les courriels, reçus ou sauvegardés depuis les ressources et services numériques de l’université sont présumés être en lien avec ses études., à défaut d’avoir été clairement identifiés comme « PRIVE » ou « privé » par l’étudiant.

Si l’étudiant reçoit par erreur un message dont il n’aurait pas dû être destinataire, toute utilisation, copie ou diffusion, même partielle de ce message est interdite. Il a l’obligation de le détruire et d’en informer immédiatement son expéditeur.

Par ailleurs, l’étudiant est informé de la mise en place de quotas individuels au niveau de chaque boîte aux lettres électronique et d’un filtrage des courriels reçus et envoyés (quotas d’envoi ou de réception, fichiers autorisés, etc.)

5.8 Médias sociaux

L'étudiant est responsable de l’information qu’il communique sur les médias sociaux tels que les forums, les blogs, réseaux sociaux, etc. Il respectera son devoir de réserve lorsqu'il s'exprimera sur ces médias. Il est donc recommandé à l'étudiant de communiquer et de publier des contenus, avec une extrême prudence.

Il est rappelé que des sanctions peuvent être appliquées en cas de divulgation d'information sensible ou d'atteinte à l'image de l’université.

Article 6. Règles d’utilisation spécifiques

6.1 Objets connectés

Les objets connectés personnels (montres, écouteurs sans fil, smartphones, tablettes, etc.) utilisés à titre privé ne doivent pas être branchés aux équipements de l’université. L'étudiant doit être conscient que l'introduction dans l'enceinte de l’université d'objets connectés peut engendrer des risques supplémentaires tels que la captation d'informations, la géolocalisation des biens et des personnes, ou la propagation de programmes malveillants.

L’étudiant est informé que l’utilisation de ce type de matériel peut être réglementée de manière plus stricte (limitation ou interdiction d’usage).

Article 7. Protection des propriétés intellectuelles, des informations et des données

7.1 Données à caractère personnel

L’étudiant s’engage à préserver les données à caractère personnel, traitées par les services numériques de l’université, conformément à la loi nº 78-17 du 6 janvier 1978 dite « informatique et libertés » modifiée par la loi nº 2004-801 du 6 août 2004 et du règlement général de protection des données du 27 avril 2016. La perte, la destruction ou la divulgation frauduleuses, accidentelles ou non autorisées de données personnelles pourraient avoir des conséquences graves pour l’université.

Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.

L’étudiant se doit de :

* respecter les finalités définies, explicites et légitimes d’un traitement comportant des données personnelles (l’utilisation de données à caractère personnel pour une finalité non autorisée constitue un « délit de détournement des données ») ;
* protéger les données personnelles afin qu’elles ne soient pas utilisées par des personnes non autorisées ou habilitées, ni divulguées, supprimées ou détruites, perdues, volées, même de manière accidentelle (cela suppose le contrôle rigoureux de la diffusion de données à caractère personnel à destinataire de tiers extérieurs à l’université) ;
* respecter et donc ne pas contourner, ni désactiver, les mesures techniques, organisationnelles et juridiques, prises par l’université pour assurer la protection des données à caractère personnel.

A ce titre, toutes les créations de fichiers comprenant ce type d'informations et demandes de traitement afférent, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, sont soumises aux formalités préalables prévues par la loi « Informatique et Libertés ».

En conséquence, tout étudiant souhaitant procéder à une telle création devra en informer préalablement le délégué à la protection des données (dpd@u-bordeaux-montaigne.fr) de l’université qui prendra les mesures nécessaires au respect des dispositions légales.

Par ailleurs, conformément aux dispositions de la loi et du règlement, chaque étudiant dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation du système d'information.

Ce droit s'exerce auprès du délégué à la protection des données (DPO) de l’établissement

7.2 Propriété intellectuelle et droit à l’image

L’étudiant s’interdit de produire, de collecter/télécharger/utiliser ou de transmettre des données, des fichiers, des logiciels, des applications, des messages, des œuvres ou des contenus protégés, quel qu’en soit le support, la nature ou la forme (par exemple photographie, dessins, écrit, enregistrement musical ou vidéo, image, logo, logiciel, etc.), qui ne soient pas dans le respect du droit de propriété intellectuelle, du droit à l’image ou du droit à la vie privée.

Chaque étudiant doit utiliser les logiciels dans les conditions des licences souscrites.

L'attention de l'étudiant est appelée sur les poursuites pénales et/ou civiles dont lui-même et/ou l'université pourraient faire l'objet du fait de la rediffusion, par quelque moyen que ce soit, de messages répréhensibles captés sur le réseau internet ou de l'utilisation, de la diffusion, voire du simple enregistrement informatique, d'œuvres ou de données en contravention avec les législations existantes ou sans l'autorisation des titulaires des droits.

Article 8. Sécurité et cyber surveillance

8.1 Signalement

L’étudiant se doit de signaler dans les plus brefs délais tout constat, tentative ou soupçon de violation de ses droits d’accès au RSSI ou correspondant SSI de proximité. La participation des étudiants à la détection d’anomalies et d’un incident de sécurité sur les services numériques est déterminante dans la rapidité de mise en œuvre des mesures de protection.

En cas de perte ou de vol de moyens d’authentification, l’étudiant doit en informer sans délai le RSSI via le formulaire « déclaration d’un incident de sécurité informatique » disponible sur l’espace étudiant.

8.2 Surveillance des ressources et services numériques

Pour garantir la sécurité des services et ressources numériques et la protection des informations nécessaires au bon fonctionnement de l’université, le RSSI peut, sans préavis, limiter ou bloquer l'accès à certains services numériques, sites Web, ressources ou à certaines parties de l’Intranet, à tous ou bien certains utilisateurs ou étudiants, pour une durée indéterminée.

Il est susceptible de mettre en œuvre des mécanismes de filtrage et d’analyser du trafic réseau, même chiffré. Des moyens de déchiffrement pourront être appliqués à l’ensemble des flux de connexion des utilisateurs et étudiants, à l’exception de ceux qui seront inclus au

sein d’une « liste blanche de sites » qui ne feront pas l’objet d’un déchiffrement de flux et de ceux dont le déchiffrement est interdit par la loi.

Il est interdit de les contourner ou de tenter de les contourner, sous peine de sanction.

8.3 Traçabilité

Pour garantir une traçabilité et être en mesure de fournir des preuves, notamment en cas d’enquête, l’université conserve, en fonction de la finalité et des durées fixées par les textes applicables, les journaux d'accès et d'utilisation générés dans les services ou ressources numériques qu’il met en œuvre. Cette conservation est réalisée dans le respect des dispositions réglementaires relatives à la protection des données personnelles.

8.4 Suivi des acquis en matière de sécurité numérique

L’université informe les étudiants par des campagnes de sensibilisation à la sécurité des services numériques et de vérification générale de leur bonne utilisation qu’il organise. Les résultats de ces campagnes seront anonymisés et ne pourront pas conduire à une sanction quelconque.

Article 9. Contrôle, maintenance et gestion des services et des ressources numeriques

9.1 Opérations de maintenance et de contrôle

Une opération de maintenance s’inscrit dans le cadre d’une opération programmée de maintien en bon état de fonctionnement des moyens considérés. La maintenance peut être opérée par des personnels internes ou des prestataires extérieurs, aussi bien sur le lieu de travail qu’à distance (télémaintenance).

Les ressources numériques de l’université font l'objet de contrôles ayant comme unique finalité d'assurer la sécurité et la continuité des ressources et des données de l’université. En cas d’événement ou d’anomalie liés à la sécurité ou à la continuité de ses systèmes, l’université s'autorise à prendre toutes les mesures nécessaires pour en identifier les causes.

L’université se réserve le droit de consulter de manière exceptionnelle le contenu des documents, fichiers ou messages, identifiés « PRIVE » ou « privé » de l’étudiant en cas de risque de mise en péril de son activité, par exemple la présence de code malveillant, en cas d’urgence ou dans le cas d’une enquête judiciaire en cours.

La collecte de données personnelles sera limitée aux informations nécessaires à la sécurité des services et des ressources numériques. Ces données sont conservées pour une durée maximale de 6 mois après collecte.

Les éléments découverts à l’occasion d'une opération de contrôle ou de maintenance sont susceptibles de constituer des moyens de preuves licites contre les agissements d'un étudiant.

L’étudiant s’engage à ne pas entraver toute opération de contrôle ou de maintenance effectuée par les services informatiques de l’université.

9.2 Logiciel anti-plagiat

L’étudiant est informé que l’université est dotée d’un logiciel de recherche automatique sur Internet de plagiat et que l’ensemble des travaux remis par les étudiants est susceptible d’être analysé.

Article 10. Responsabilités et sanctions

Le non-respect des règles d’utilisation et des mesures de sécurité figurant dans la présente charte est susceptible de justifier la suspension immédiate de l’utilisation de tout ou partie des services et ressources numériques, et/ou l’engagement de poursuites disciplinaires adaptées à la gravité des agissements constatés, sans préjudice d'éventuelles actions pénales ou civiles à l’encontre de l’étudiant.