Sciences Po Bordeaux

Charte des usages numériques

NOM :

Prénom :

Je reconnais avoir pris connaissance de la charte des usages numériques qui m'a été adressée. Je respecte cette charte pour toute la durée de mon engagement auprès de l'Institut d'Études Politiques de Bordeaux. Je m'engage à signaler tout usage non conforme de cette charte porté à ma connaissance.

Le :

Pour valoir acte d'engagement

Signature :

Sciences Po Bordeaux

Charte des usages numériques

Sciences Po Bordeaux en tant que membre de Réaumur (cellule réseau universitaire) est tenu de respecter la charte suivante :

RÈGLEMENT INTÉRIEUR DU RÉSEAU RÉAUMUR

Version 2 – CA du 10/11/2004

Le réseau RÉAUMUR ne doit être utilisé qu'à des fins professionnelles d'enseignement et de recherche.

Ce réseau ne constitue en aucun cas un accès banalisé à l'Internet tel que peut en offrir un prestataire de services.

Le règlement intérieur précise les droits, devoirs, responsabilités de chacun pour l'utilisation du réseau RÉAUMUR.

Il complète et précise la charte du réseau RENATER, laquelle s'applique entièrement à RÉAUMUR.

Il n'est pas exclusif de règles d'utilisation des ressources informatiques énoncées par les organismes ou laboratoires.

Il définit les règles d'utilisation et d'administration de l'ensemble des systèmes connectés à RÉAUMUR.

Il précise également les règles d'utilisation des équipements informatiques distants accessibles à partir de RÉAUMUR, à travers le réseau régional ESRA, le réseau national RENATER, le réseau INTERNET mondial, ou tout autre moyen.

Tout signataire du document intitulé : " *Engagement des utilisateurs du réseau RÉAUMUR* " est tenu de se conformer au présent règlement intérieur, conformément à l'article I du document précité.

1.1. Les moyens informatiques concernés

Le règlement concerne l'ensemble des équipements informatiques connectés directement ou indirectement à RÉAUMUR.

Ils comprennent notamment les serveurs, stations de travail, micro-ordinateurs, ordinateurs portables ou tout autre équipement mobile communiquant (PDA, téléphone, ...), terminaux des salles en libre-service (travaux pratiques enseignements, bibliothèques, ...), des laboratoires, écoles, instituts, services administratifs...

1.2. Les utilisateurs

Toute personne utilisant un équipement connecté à RÉAUMUR est considérée comme utilisateur de RÉAUMUR.

L'accès aux moyens informatiques est donné par le service auquel on est rattaché, à titre temporaire. Il sera retiré dans le cas d'un comportement en désaccord avec les principes minima énoncés dans ce règlement et dans l'engagement des utilisateurs.

1.3. Le responsable sécurité, les administrateurs

Chaque machine connectée est gérée et contrôlée par un responsable sécurité connu de la cellule RÉAUMUR.

Le responsable sécurité peut déléguer la gestion des machines à des administrateurs.

Le responsable sécurité veille au bon respect des règles d'exploitation.

Il procède aux enquêtes et investigations nécessaires et répond aux besoins d'éventuelles procédures disciplinaires ou judiciaires.

2.1. Respect de l'identité

Le droit d'accès à un système est personnel et incessible. Notamment : les mots de passe ne doivent être ni communiqués, ni stockés.

En conséquence, il est interdit :

a) d'utiliser le compte d'un tiers,

b) d'envoyer, ou tenter d'envoyer des messages ou des courriers électroniques anonymes ou sous une identité usurpée.

2.2. Respect des règles de sécurité

L'utilisateur doit se mettre en conformité avec les mesures adoptées par le responsable sécurité de RÉAUMUR, notamment en matière de gestion de mot de passe.

Il doit signaler au responsable sécurité de sa machine toute tentative de violation ou d'effraction sur un compte, sur des données ou sur l'intégrité du système.

2.3. Respect de la confidentialité

Les données contenues dans des fichiers ou transmises sur les réseaux par des utilisateurs ou des administrateurs doivent être considérées comme privées, qu'elles soient ou non accessibles par les autres utilisateurs.

La possibilité d'accéder à un fichier n'implique pas le droit de le consulter.

Le fait d'avoir la possibilité de modifier un fichier n'implique pas que l'on ait le droit de l'altérer.

2.4. Respect de l'intégrité des systèmes

L'utilisateur ne doit en aucun cas modifier :

- le contenu des fichiers système,
- le contenu des fichiers de configuration réseau,
- le contenu des fichiers relatifs à la sécurité des machines ou équipements réseau.

L'utilisateur ne doit en aucun cas utiliser ou tenter d'utiliser les privilèges d'administration du système.

L'utilisation, le stockage de logiciels pouvant porter gravement atteinte à la sécurité des systèmes (virus, chevaux de Troie, vers, logiciel d'espionnage de lignes de communication...) sont interdits.

Un utilisateur qui pense avoir de bonnes raisons de faire des expériences relatives à la sécurité des moyens informatiques **doit discuter de ce projet avec le responsable sécurité de RÉAUMUR.**

2.5. Respect des restrictions légales d'utilisation

Les conditions d'acquisition de certains logiciels restreignent leurs conditions d'utilisation. Les réseaux ne doivent en aucun cas être utilisés pour outre passer ces conditions d'utilisation.

De même, il est nécessaire de respecter les règles qui régissent la propriété intellectuelle et artistique.

L'utilisateur a le droit de demander à un responsable sécurité ou à un administrateur de prendre les mesures appropriées pour mettre fin à tout abus dont il serait victime.

L'utilisateur a le droit et le devoir d'utiliser tous les moyens mis à sa disposition par le système d'exploitation pour garantir la confidentialité de ses données, restrictions de droits d'accès, cryptage, sauvegarde sur support amovible...

Les responsables sécurité et les administrateurs doivent informer tout utilisateur potentiel des règles édictées par le présent document.

La signature par l'utilisateur de l' « Engagement des utilisateurs du réseau RÉAUMUR », les exonère de cette obligation.

Les responsables sécurité appliquent et font appliquer par les administrateurs, les consignes de sécurité préconisées par la cellule réseau RÉAUMUR.

Les responsables sécurité informent le responsable sécurité de RÉAUMUR et leurs autorités hiérarchiques des problèmes de sécurité constatés. Ils collaborent aux enquêtes nécessaires pour établir les responsabilités.

Les comptes collectifs ouverts par les administrateurs, à titre exceptionnel (cf. article III.2 de l' «Engagement des utilisateurs du réseau RÉAUMUR») feront l'objet d'une évaluation par le responsable sécurité de RÉAUMUR.

Les responsables sécurité, et les administrateurs doivent impérativement respecter la confidentialité des fichiers des utilisateurs ainsi que de leur courrier électronique.

Les responsables sécurité, et les administrateurs ont le devoir d'informer les utilisateurs et la cellule réseau RÉAUMUR par les moyens les plus appropriés (circulaires, courrier électronique...) de toute intervention qu'ils seraient amenés à faire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques et plus particulièrement du service réseau. Ceci concerne notamment les interconnexions de réseaux, les équipements réseaux, le service du courrier électronique.

Les responsables sécurité et les administrateurs doivent prendre les mesures nécessaires au bon fonctionnement du réseau et au respect des règles d'utilisation ; dans ce cadre, ils peuvent avoir à examiner des fichiers privés ou des courriers, à fins de diagnostic et d'enquête, dans le respect de la confidentialité des informations privées des utilisateurs.

À titre conservatoire, ils peuvent prendre des mesures de restriction d'utilisation d'un compte ou d'un service.

Le responsable administratif du laboratoire ou du service définit en accord avec la cellule réseau RÉAUMUR les éventuelles modalités particulières d'accès au réseau. **Elles nécessitent la conclusion d'une convention entre les parties.**

Le responsable administratif du laboratoire ou du service engage les moyens financiers nécessaires à la mise en place et au fonctionnement des services utilisés par ce laboratoire ou ce service.

ANNEXE

PRINCIPAUX TEXTES RÉPRIMANT LES ATTEINTES À LA SÉCURITE DES MOYENS INFORMATIQUES

Version 2 – CA du 10/11/2004

Tout utilisateur autorisé ou non encourt, en plus des sanctions disciplinaires, des sanctions pénales et civiles, prévues par plusieurs textes législatifs, en raison de comportements liés à l'utilisation de l'informatique. En particulier la loi réglemente la fraude informatique (Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique), la protection des logiciels et des progiciels (Loi n° 2004-204 du 9 mars 2004), la protection des fichiers nominatifs (Loi n°2004-801 du 6 août 2004 relative à l'informatique, aux fichiers et aux libertés)

Ces textes législatifs définissent un certain nombre de délits et de peines.

À titre d'exemple :

Code Pénal – Articles L323-1 à L323-3-1

Article L323-1 : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.
Article L323-2 : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
Article L323-3 : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
Article L323-3-1 : Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles L323-1 à L323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité
Code de la Propriété Intellectuelle - Articles. L335-2 et suivants

La reproduction d'un logiciel autre qu'une copie de sauvegarde, de même que l'utilisation d'un logiciel non expressément autorisé, sont passibles d'une peine d'emprisonnement de 2 ans et d'une amende de 150 000 euros.
De même, les bases de données bénéficient également d'un régime de protection particulier prévu par le Code de la Propriété Intellectuelle (Art. L341-1 et suivants du C.P.I.).

Code Pénal – Article L226-16

Article L226-16 : Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article L45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

ENGAGEMENT DES UTILISATEURS DU RESEAU RÉAUMUR

Version 2 – CA du 10/11/2004

INTRODUCTION

Tout utilisateur d'un équipement informatique connecté à RÉAUMUR, est informé que ce réseau est destiné exclusivement à véhiculer le trafic engendré par des activités de recherche, de développement technologique et d'enseignement supérieur. Les activités d'administration et de gestion des centres de recherche ou d'enseignement supérieur sont assimilées à la recherche ou à l'enseignement supérieur.

ARTICLE I

Tout utilisateur d'équipement informatique connecté à RÉAUMUR s'engage à prendre connaissance du Règlement Intérieur de ce Réseau et à s'y conformer. De la même manière, il reconnaît avoir pris connaissance des recommandations jointes à cet engagement.

ARTICLE II

Sont passibles de poursuites disciplinaires, civiles, pénales, tous les actes réalisés dans l'intention de nuire ou susceptibles de nuire à tout utilisateur d'un équipement informatique au moyen de RÉAUMUR.

ARTICLE III

Tout compte identifie un utilisateur, personne physique, responsable de l'utilisation de ce compte.
Toute usurpation de compte est susceptible de poursuites. - A titre exceptionnel, des comptes collectifs peuvent être ouverts sous la responsabilité d'une personne prenant à sa charge les responsabilités liées à la nature de ce compte.
Tout utilisateur d'un applicatif d'accès banalisé (exemple : accès au catalogue des bibliothèques, au service de la scolarité...) s'engage à rester dans les limites de cet applicatif.

ARTICLE IV

Tout utilisateur s'engage à ne pas prêter son compte et à ne pas le rendre accessible par négligence. Il se met en conformité avec les mesures adoptées par le responsable Sécurité de RÉAUMUR, notamment en matière de gestion de mots de passe.

ARTICLE V

Chaque équipement connecté à RÉAUMUR est contrôlé par un responsable Sécurité. Ce dernier dispose à cette fin des moyens d'investigations nécessaires lui permettant d'examiner éventuellement les données des utilisateurs dans le respect de la confidentialité.

ARTICLE VI

Dans les conditions fixées par le Règlement Intérieur concernant le fonctionnement de RÉAUMUR, le responsable Sécurité doit informer les instances concernées de toutes infractions ou violations constatées ou suspectées.

ARTICLE VII

Tout utilisateur s'engage à signaler au responsable Sécurité de sa machine, toute tentative de violation ou d'effraction sur son compte, ses données et l'intégrité du système. La non observation de cet article peut entraîner des restrictions d'utilisations à titre conservatoire, pour les besoins de l'enquête.

ARTICLE VIII

Tout utilisateur d'un équipement informatique connecté à RÉAUMUR s'interdit toute utilisation d'une machine locale ou distante sur laquelle il ne possède pas de numéro de compte (à l'exception des services anonymes. Exemple : ftp anonymous...). Des poursuites pénales pourront être engagées en application de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (articles L323-1 à L323-3-1 du Code Pénal)

ARTICLE IV

Chaque utilisateur est responsable de l'utilisation des logiciels et matériels mis à sa disposition.
Il est rappelé que l'usage et l'installation de logiciels (programme, plug-in, agent, démon…) même libre de droit est soumis à autorisation écrite du service informatique copie devant être remise au secrétariat général.

Sciences Po Bordeaux se réserve le droit de suspendre l'accès aux ressources de toute personne contrevenant aux règles établies, et de prendre toute mesure administrative qu'elle jure adéquate.
L'entité ne peut être tenue responsable en cas en cas d'indisponibilité du système et de perte de données et / ou de temps dans le cadre de l'utilisation des ressources informatiques. De plus l'entité encourage les utilisateurs à mettre en oeuvre tout moyen de sauvegarde personnel. L'effacement ou la perte de données stockées ou utilisées sur le système ne relève pas de la responsabilité de l'entité.

Recommandation d'utilisation du réseau

Quelques exemples de pratiques inacceptables

Version 2 – CA du 10/11/2004

Les recommandations présentées ci-dessous ne constituent pas une liste exhaustive mais seulement un ensemble d'informations concrètes.

LE RÉSEAU EST DESTINÉ EXCLUSIVEMENT À DES FINS PROFESSIONNELLES D'ENSEIGNEMENT ET DE RECHERCHE.

LE RESEAU RÉAUMUR N'EST PAS UN ACCÈS BANALISÉ À INTERNET.

Parmi les pratiques peu recommandables et donc inacceptables, on peut citer les exemples suivants :

1. Donner ses mots de passe ou prêter ses comptes (ex: par l'intermédiaire de rhost).
2. Laisser son poste de travail sans surveillance.
3. Rechercher ou transférer ou tenter de par quelque moyen que ce soit (ex: P2P, ftp, fsp, irc/dcc, échanges MSN Messenger, mail, www...).
   - › toute copie frauduleuse de documents ou logiciels (ex: logiciel piraté, warez),
   - › tout document facilitant le piratage de logiciel (ex: cracks, num. de série),
   - › tout document ou logiciel servant à pirater les machines (ex : scanner, sniffer, cracker, rootkit, ...)
   - › tout document aidant au développement de virus.
4. Violer les règles d'utilisation de certains documents (ex : diffuser par le WEB des textes, sons et images soumis aux droits d'auteurs et de propriété intellectuelle et artistique).
5. Utiliser des logiciels exclusivement employés pour récupérer des documents volumineux et non professionnels, voire illégaux (P2P type Gnutella, Kazaa, Edonkey, SoulSeek, PeerEnabler,...).
6. Chercher à obtenir ou utiliser des accès illégaux sur une machine même sans intention de nuire.
7. Ne pas respecter la législation sur les moyens de chiffrement.
8. Utiliser/installer le logiciel Skype interdit par le MENESR.

Si vous pensez avoir de bonnes raisons d'effectuer une action mentionnée ci-dessus vous devez IMPÉRATIVEMENT en demander l'autorisation à vos responsables puis à la cellule RÉAUMUR. Dans le cas contraire, vous seriez considéré comme ayant délibérément enfreint le règlement avec tous les risques et désagréments que cela comporte.

La Cellule RÉAUMUR et Sciences Po Bordeaux effectue les contrôles permettant de vérifier le respect de ces règles.

→ Pour plus d'informations : http://www.reaumur.u-bordeaux.fr

Sciences Po Bordeaux

Charte anti-plagiat

D'un point de vue juridique, le plagiat est une atteinte au droit d'auteur et à la propriété intellectuelle, il peut être assimilé à un délit de contrefaçon. C'est aussi une faute disciplinaire, susceptible d'entraîner une sanction.

Afin de détecter les éventuels plagiats l'IEP de Bordeaux se dote d'outils informatiques performants et s'abonne à un logiciel de détection des plagiats. Le présent document a pour but d'expliciter les règles concernant le plagiat afin de les adapter au développement d'internet et des TIC et de permettre aux étudiants de se mettre en conformité avec la réglementation en vigueur.

Pourquoi et comment éviter le plagiat ?

Le développement d'internet, source inépuisable de documentation et de données diverses, a amené un développement parallèle du plagiat, sous différentes formes. La très grande accessibilité des sources, les facilités du « copier-coller », ont facilité des pratiques nouvelles ; la limite entre l'inspiration, l'imitation et le plagiat devient parfois difficile à fixer. Il semble donc nécessaire de définir ce qui est permis et ce qui constitue une fraude.

Pour résumer, le fait d'omettre de citer ses sources [qu'elles viennent d'internet, de document papier ou autre] est un acte de plagiat. Il est interdit d'utiliser, en totalité ou partiellement, un texte d'autrui en le faisant passer pour le sien [même avec son autorisation] ou sans indication de référence. Il est aussi interdit de présenter, pour des évaluations différentes [sauf autorisation expresse], un même travail, que ce soit intégralement ou partiellement, dans différents cours.

Chaque travail demandé doit être original.

Il n'est pas interdit de reprendre les idées d'un auteur, c'est même le propre d'un travail universitaire d'utiliser les travaux des différents auteurs, de s'appuyer sur eux et de les discuter, mais il faut le faire correctement.

Il est absolument nécessaire de citer ses sources.

Pour permettre au lecteur de vérifier l'exactitude des données rapportées ou du texte cité, ou encore de voir le texte cité dans son contexte.

Pour faciliter le repérage des sources par le lecteur.

Pour valoriser son propre travail en l'insérant dans les différentes sources extérieures, dans des courants de pensée situés dans le temps ou dans l'espace.

Pour citer ses sources on peut utiliser la technique de la citation, qui doit obéir à des règles précises.

« La citation doit être reproduite textuellement, ce qui veut dire qu'on doit aussi retranscrire tel quel la ponctuation, les majuscules, les fautes, les coquilles ainsi que la mise en forme [gras, italique, souligné]. On met ces mots entre guillemets [«…»] ou en retrait lorsque la citation fait plus de trois lignes : tout terme douteux [faute, coquille, etc.] doit être suivi de l'adverbe sic entre crochets [sic].

On peut citer un passage en langue étrangère si on sait que les lecteurs maîtrisent la langue de l'extrait. On n'a alors qu'à mettre le passage cité en italique et entre guillemets [«…»]. Si on pense que la langue originale ne peut pas être comprise par les lecteurs, on doit essayer de trouver une traduction déjà publiée de l'extrait. Il faut s'assurer d'indiquer dans la référence le nom du traducteur ainsi que les dates de publication et de traduction. Si aucune traduction n'a été publiée, on doit traduire soi-même l'extrait. Il suffit de mettre sa traduction entre guillemets [«…»] et d'indiquer la mention *Notre traduction* entre crochets [ ]. Toute modification d'une citation doit être signalée par des crochets [ ].

Lorsqu'on veut citer un passage et que l'on n'a pas accès à la source originale, on doit mentionner non seulement la source d'où est tirée la citation, mais également la source originale. Généralement, on utilise des formules comme « cité dans » ou « cité par ». Pour les tableaux ou graphiques, on procèdera de la même façon, mais on utilisera la formule « tiré de ». »

Source : http://www.bibliotheques.uqam.ca/recherche/plagiat/citer.html

Bien entendu, il faut toujours accompagner la citation d'une référence complète.

L'étudiant peut aussi être amené à utiliser la paraphrase, pour présenter, avec ses propres mots, en les intégrant dans son texte, les idées d'un auteur. Il ne devra jamais oublier, même s'il utilise ses propres mots et pas ceux de l'auteur, de citer explicitement l'auteur, d'indiquer clairement ses sources. S'il conserve quelques passages de l'auteur, même quelques mots, il doit considérer qu'il s'agit d'une citation et donc les mettre entre guillemets. La paraphrase n'est pas interdite, elle permet à l'étudiant de montrer qu'il a parfaitement compris la pensée de l'auteur et qu'il sait l'utiliser, mais il est **absolument nécessaire de faire référence au document d'où provient l'information**.

L'étudiant qui utilise la pensée d'un auteur pour l'intégrer dans son texte [en prenant soin d'y faire une référence explicite] ne peut se contenter de remplacer certains termes par des synonymes. Il doit réellement faire un travail d'écriture ; dans le cas contraire, il est préférable de s'en tenir à une citation.

Quelques exemples de plagiat, tirés du site des bibliothèques de l'université de Québec à Montréal :

- Copier textuellement un passage d'un livre, d'une revue ou d'une page Web sans le mettre entre guillemets et/ou sans en mentionner la source.
- Insérer dans un travail des images, des graphiques, des données, etc. provenant de sources externes sans indiquer la provenance.
- Résumer l'idée originale d'un auteur en l'exprimant dans ses propres mots, mais en omettant d'en indiquer la source.
- Traduire partiellement ou totalement un texte sans en mentionner la provenance.
- Réutiliser un travail produit dans un autre cours sans avoir obtenu au préalable l'accord du professeur.
- Utiliser le travail d'une autre personne et le présenter comme le sien [et ce, même si cette personne a donné son accord].
- Acheter un travail sur le Web.

Sanctions

Le plagiat est une fraude grave relevant de la section disciplinaire de l'IEP qui pourra prononcer une des sanctions suivantes :

- Avertissement.
- Blâme.
- Zéro à l'évaluation en cause, avec possibilité de rattrapage.
- Zéro à l'évaluation en cause, sans possibilité de rattrapage.
- Zéro au module d'enseignement concerné [par ex. : cours, séminaire, conférence…].
- Zéro à la session d'examen.
- Suspension de l'IEP.
- Exclusion définitive de l'IEP.
- Suspension de tout établissement public d'enseignement supérieur.
- Exclusion définitive de tout établissement public d'enseignement supérieur.

Le plagiat est un délit pouvant être poursuivi devant les juridictions compétentes. Une action en justice doit être réservée à des cas exceptionnels, mais Sciences Po Bordeaux n'en exclut pas la possibilité.

Sciences Po Bordeaux

Formulaire d'engagement anti-plagiat

Je soussigné·e _____

étudiant·e en _____ à Sciences Po Bordeaux

- déclare avoir pris connaissance de la charte anti-plagiat annexée au *Règlement des études* de Sciences Po Bordeaux sur décision du Conseil d'administration en date du 13 juin 2008 ;
- reconnaît que le plagiat constitue une atteinte au droit d'auteur et à la propriété intellectuelle, assimilable à un délit de contrefaçon, ainsi qu'une faute disciplinaire incompatible avec les principes pédagogiques en vigueur au sein de Sciences Po Bordeaux ;
- autorise les équipes pédagogiques de Sciences Po Bordeaux à soumettre mes travaux écrits à un examen comparatif auprès de Compilatio.net, service en ligne de détection et de prévention du plagiat [1] ;
- assume en conséquence les éventuelles sanctions disciplinaires, voire judiciaires, auxquelles un recours à cette pratique frauduleuse est susceptible de m'exposer.

Cet engagement vaut pour l'intégralité de la scolarité à Sciences Po Bordeaux. Il s'applique à l'ensemble des travaux soumis à évaluation dans le cadre de la scolarité.

Fait à .....

Le ..... / ..... / 20.....

Signature

[1] *Pour tout renseignement sur ce service : www.compilatio.net*