Institut Régional Supérieur du Travail Éducatif et Social de Bourgogne

Charte de l'utilisateur des moyens et ressources informatiques de l'IRTESS de Bourgogne

Version actualisée le 23 février 2024

Préambule

Les techniques d'information et de communication (TIC) sont de plus en plus présentes dans les environnements de travail comme dans la vie quotidienne, avec leurs avantages, leurs limites et les risques qui les accompagnent…

Le développement des TIC en ont fait un outil de plus en plus nécessaire à l'exercice d'une activité professionnelle et un moyen incontournable de la formation.

Les avantages attendus de ces nouvelles technologies passent par une bonne utilisation des moyens et ressources informatiques. C'est l'objet de cette charte à destination de l'ensemble des utilisateurs de l'IRTESS de Bourgogne.

Les règles et obligations de la présente charte s'appliquent à tout utilisateur de l'ensemble des moyens et ressources informatiques de l'IRTESS (annexe n°1), dans le respect des fonctions, des obligations et des droits de chacun, ainsi que du cadre légal et réglementaire de l'IRTESS et celui du Règlement Général de la Protection des Données (loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, qui a modifié la loi Informatique et Libertés afin de mettre en conformité le droit national avec le cadre juridique européen du règlement général de la protection des données).

La présente charte est aussi un code de bonne conduite permettant une utilisation optimale des ressources informatiques de l'IRTESS en accord avec les règles de courtoisie et de respect d'autrui.

L'élaboration de la présente charte fait l'objet de mises à jour en fonction de l'évolution du système informatique, des logiciels et de la réglementation.

La présente charte comporte des annexes.

I. L'autorisation d'accès aux moyens et ressources informatiques

Les locaux de l'IRTESS sont protégés par une alarme anti-intrusion. Les bureaux et salles fermés à clé si non occupés et font l'objet de l'installation de portables dans les salles limitées au temps d'utilisation. L'ensemble du système informatique de l'IRTESS est en infogérance chez PSI notre prestataire (voir annexe n°2 « Politique de traitement des données personnelles ».)

La gestion informatique est confiée par le prestataire de service PSI qui dispose d'une politique de sécurité de traitement des données personnelles complète.

L'autorisation d'accès aux moyens et ressources informatiques est accordée par la Direction de l'IRTESS à chaque utilisateur, de manière personnelle et nominative (nom, prénom, fonction). Cette autorisation ne peut en aucun cas être cédée, même temporairement ou gratuitement.

Cela se concrétise notamment par :

- L'octroi de codes de connexion et mots de passe associés, strictement personnels et confidentiels ;
- L'attribution d'une Licence Office 365 pour chaque étudiant et stagiaire ;
- L'accès à des espaces de travail.

Concernant les salariés de l'IRTESS et les intervenants occasionnels :

- L'espace de bureau de l'ordinateur portable ne doit pas conserver vos fichiers professionnels : c'est seulement sur la session qui a été attribuée que l'ensemble des dossiers doivent être positionnés ;
- Les intervenants occasionnels auxquels ne doivent pas laisser des clés USB ou des CD-ROM après usage : en cas de constat, ces matériels abandonnés seront systématiquement détruits ;

Retrait et suspension de l'autorisation d'accès

L'autorisation d'accès est définitivement retirée à la fin de l'activité professionnelle ou de formation de l'utilisateur. Elle peut être temporairement suspendue en cas de non-respect de la présente charte.

II. Conditions d'utilisation des moyens et ressources informatiques

Chaque utilisateur contribue à la sécurité et à l'intégrité des moyens informatiques en respectant la charte et en ayant une utilisation loyale de ces moyens, il s'engage à respecter les consignes et préconisations de l'administrateur.

D'une façon générale, la possibilité d'accéder techniquement à une ressource n'implique pas qu'on ait le droit de le faire, de même les fichiers d'un utilisateur doivent être considérés comme privés, même s'ils sont accessibles, techniquement par d'autres utilisateurs.

Chaque utilisateur participe à la sécurité de l'environnement informatique en respectant certaines règles de base :

- L'accès au paramétrage est réservé à direction de l'IRTESS habilitée ;
- Les codes de connexion et mots de passe ne doivent pas être communiqués à un tiers et être gardés en lieu sûr. Les mots de passe sont modifiés tous les trois mois ;
- Une session de travail doit être fermée lorsque l'on quitte son poste de travail ;
- L'utilisateur doit s'assurer, de l'origine de tout message électronique et de fichier avant introduction dans le système, et ne jamais ouvrir une pièce jointe dont l'origine est incertaine ou pouvant contenir des commandes (extension de fichier : .exe, .bat, .pif, .vbs… ou double extension :foto.gif.exe...) ;
- L'utilisateur ne doit pas rester connecté au wifi lorsque ce n'est plus nécessaire,

- Aucun périphérique ne doit être ajouté et/ou débranché, le matériel informatique ne doit pas être déplacé sans autorisation.

L'utilisateur s'engage à :

1. Une mise en œuvre des moyens et ressources informatiques de l'IRTESS sous son propre identifiant :

   – Ne pas chercher à masquer son identité ou usurper celle d'un autre utilisateur ;
   – Signaler toute perte de son code d'accès ;
   – Ne pas donner accès au réseau à des tiers non autorisés, que ce soit à titre commercial, rémunéré ou gratuitement ;
   – Protéger son propre espace de travail de toute intervention d'un tiers de manière à éviter les perturbations du réseau ;
   – Ne pas tenter de lire, modifier, copier ou détruire d'autres fichiers que ceux qui lui appartiennent, directement ou indirectement.
   – Tout incident sur le matériel ou disparition du matériel informatique doit être signalé à la direction de l'IRTESS,

2. Une utilisation des moyens et ressources informatiques de l'IRTESS à des fins strictement professionnelles conformes à leur finalité (enseignement, recherche, diffusion d'informations pédagogiques ou administratives) :

   – Accéder, créer, véhiculer, mettre à disposition sur le réseau, seulement des ressources et des données licites ;
   – Les forums de discussion, les tchats sont autorisés uniquement dans le cadre pédagogique validé par les formateurs et dans le respect des personnes.
   – Respecter le droit à l'image. Le « droit à l'image » permet à toute personne de faire respecter son droit à la vie privée. Un internaute pourra par exemple refuser que son image soit reproduite ou diffusée sur n'importe quel support sans son autorisation expresse.

3. Une utilisation rationnelle et loyale des moyens et ressources informatiques de l'IRTESS :

   – Éviter toute consommation abusive des ressources téléchargement de fichiers de taille importante, manipulation d'images, de son, de vidéos et toute autre pratique dite d' « aspiration de données » ;
   – Prévenir et s'abstenir de toute activité malveillante destinée à perturber ou porter atteinte au réseau.

4. Respecter les dispositions du Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) et à la libre circulation de ces données. Les utilisateurs ne sont pas autorisés à photocopier ou/et enregistrer les données personnelles en dehors des salariés ayant précisé des finalités dans le registre de traitement des données personnelles. Tous les utilisateurs s'engagent à respecter ces obligations au risque d'encourir une sanction. L'IRTESS dispose de fiches spécifiques en cas de violation des données personnelles ou analyses d'impact relatives à la protection des données personnelles.

   Les utilisateurs, notamment les salariés, ont signé leur contrat dans lequel une clause de confidentialité et de respect des données dans le cadre de la protection des données personnelles.

   Vous pouvez exercer votre droit d'accès, de rectification et d'effacement aux données personnelles vous concernant, en contactant la direction de l'IRTESS.

   Pour toute réclamation concernant l'usage irrégulier de vos données personnelles, vous pouvez contacter notre délégué à la protection des données (DPO) par mail : dpo@irtess.fr ou à l'adresse postale de l'RTESS à l'attention du DPO.

III. Administration du réseau informatique de l'IRTESS

Afin de permettre une utilisation optimale et correcte des moyens informatiques, d'assurer la sécurité du réseau, ainsi que des informations et des données contenues dans le réseau, la direction de l'IRTESS travaille conjointement et régulièrement avec le prestataire de service PSI.

Afin de remplir ses missions et dans la limite de ces dernières, la direction de l'IRTESS possède des droits étendus sur l'utilisation des moyens informatiques. La direction de l'IRTESS est tenue à un strict respect des obligations de discrétion professionnelle, concernant les informations qu'elle aurait été amenée à connaître dans le cadre de sa fonction et, en particulier, lorsque celles-ci sont couvertes par le secret de la correspondance ; elle ne saurait, à ce titre, être contrainte de divulguer ces informations, sauf dispositions d'ordre public contraires.

Néanmoins, il est rappelé que la confidentialité et l'intégrité des données véhiculées sur Internet ne sont jamais complètement garanties.
La direction de l'IRTESS est soumise au devoir de réserve en référence à l'article 226-13 du code pénal pour toutes informations à caractère confidentiel concernant un utilisateur, qu'elle serait amenée à connaître involontairement dans l'exercice de sa mission.

IV. Sécurité et contrôle des moyens informatiques et de leur utilisation

L'IRTESS a prévu dans sa mise en conformité du RGPD un plan d'action, qui prévoit dans la première étape, un rappel de la réglementation du RGPD à l'ensemble des utilisateurs.

Cette première étape mentionne :

- Rappeler et sensibiliser les salariés et étudiants des principes généraux du RGPD chaque année. Responsabiliser les salariés sur le traitement dès la conception du projet et tout au long du cycle de vie des données traitées. Une formation MOOC proposée par l'Agence nationale de sécurité informatique a été indiqué à l'ensemble du personnel. Le DPD se forme régulièrement sur le RGPD via les délibérations de la CNIL, les formations proposées en ligne et les ouvrages spécifiquement dédiés à ses fonctions.
- Rencontrer les équipes une à deux fois par année avec un référent RGPD et le DPD (veille juridique : lecture régulière des délibérations de la CNIL). Des rencontres entre les équipes et le DPD se déclenchent de façon spontanée selon les demandes et besoins afin de garantir la mise en conformité du RGPD à l'IRTESS.
- Adresser des notes d'information régulièrement sur les mesures de la réglementation (application concrète, analyse des risques et identification des violations des données avec document type et date) dans des circonstances ou conditions particulières.
- Répondre aux besoins exprimés par les salariés sur des moyens de protection des données personnelles, au regard des activités respectives de chacun ou sur le développement de nouveaux procédés innovants en la matière.

Le DPD tient un cahier de bord, sous forme de tableau, des rencontres avec les utilisateurs concernant des informations et sensibilisations en matière de RGPD, ceci sur différentes thématiques recensées comme les durées de conservations, les archives pédagogiques, les demandes de consentement, rappels des grands principes du RGPD. Des rencontres régulières sont prévues tout au long de l'année sur des thématiques spécifiques avec l'ensemble des équipes de l'IRTESS, ceci afin d'approfondir les connaissances sur le RGPD.

L'IRTESS met en œuvre, autant que faire se peut, les moyens de sécurité, de contrôle et de sauvegarde nécessaires à l'intégrité et à la maintenance des moyens informatiques et notamment un système antivirus, pare-feu soit par ses propres moyens, soit par les services de l'organisme prestataire PSI. Le prestataire de service met en œuvre les moyens nécessaires afin de garantir la confidentialité, l'intégrité, la disponibilité des systèmes et des services de traitement.

Le système informatique de l'IRTESS est sécurisé et garanti par la politique de sécurité du prestataire de service :

- Authentification par un identifiant unique et strictement confidentiel à l'entrée sur le réseau sécurisé ; droits en rapport avec le statut ou la fonction de l'utilisateur ;

- Habilitations gérées : individualisées, accès selon les fonctions des salariés ;

- Traçage des accès et gestion les incidents : log, journalisation ;

- Sécurisation des postes de travail ; équipements inventoriés et étiquetés ; fiches des incidents relevés (intrusion illégale, piratage, perte ou vol de portable) ;

- Protection du réseau informatique : pare-feux certifiés par L'ANSSI en protection et antivirus et gestion des flux identifiés et dédiés à L'IRTESS ;

- Mises à jour de toutes les applications utilisées par l'IRTESS ;

-Sécurité des serveurs dédiés exclusivement à l'IRTESS : infrastructure de serveur redondante ; politique de sauvegarde journalière et d'externalisation testée régulièrement, cloisonnement des données ;

- Règles d'alertes d'incidents et procédures spécifique visant à garantir l'intégrité des données informatiques et à rétablir le bon fonctionnement de l'ensemble du système informatique de l'IRTESS ;

- Sauvegarde régulière et continuité d'activité prévues : plan de sauvegarde à plusieurs niveaux ;

- Archive numérique sécurisée dans le cadre du réseau ;

- Une purge des ordinateurs est réalisée lorsqu'un utilisateur salarié remet définitivement le matériel au service logistique ;

- Sauvegarde physique sur bandes régulières en plus du plan de sauvegardes classiques.

Le système de sauvegarde des serveurs est destiné à prévenir d'éventuelles défaillances matérielles (destruction d'un serveur par exemple) ; ces sauvegardes ne se substituent pas à l'enregistrement ordonné des données de chacun. Elles n'ont pas vocation à restaurer des données dans le cas d'erreurs de manipulation.

Les conditions de traitement et de conservation éventuels des fichiers (journalisation, log) seront précisées autant que nécessaire en annexe à la présente charte.

Afin de garantir l'intégrité et la bonne utilisation des moyens informatiques, la Direction de l'IRTESS peut procéder à des contrôles dans le respect de la loi et de la réglementation en vigueur, notamment en ce qui concerne le respect de la vie privée et le secret de la correspondance.

En cas d'utilisation incorrecte des moyens informatiques, l'utilisateur concerné en sera informé par la Direction et pourra voir son autorisation d'accès provisoirement suspendue. Tout agissement fautif pourra donner lieu à des sanctions telles que prévues au règlement intérieur.

V. Validité de la charte

La présente charte entre en vigueur à compter du 25 janvier 2023 et remplace la précédente.

Annexe n° 1 : Liste des moyens et ressources informatiques de l'IRTESS concernés par la charte de l'utilisateur
Annexe n° 2 : Liste informative des infractions susceptibles d'être commises
Annexe n° 3 : Fiche d'analyse d'impact des données personnelles
Annexe n° 4 : Fiche type de violation des données personnelles
Annexe n° 5 : Tableau des suivis des réunions d'équipes dans la mise en conformité du RGPD
Annexe n° 6 : Politique de traitement des données personnelles du prestataire de service PSI

ANNEXE n° 1

Liste des moyens et ressources informatiques de l'IRTESS concernés par la charte de l'utilisateur

- Ordinateurs fixes ou portables et leurs périphériques, copieurs, téléphones fixes et mobiles, tableaux numériques ;

- Ensemble des équipements de transmission : commutateurs, routeurs et autres ;

- Infrastructure de liaison du réseau : wifi, câbles, fibre optique, point de connexion, circuit électrique protégé, locaux techniques ;

- Environnement Office 365, ensemble des logiciels et systèmes d'exploitation ;

- Tout moyen auquel il est possible d'accéder à distance, directement ou en cascade à partir d'internet, administré par l'IRTESS.

ANNEXE n° 2

Liste informative
des infractions susceptibles d'être commises

1. Infractions prévues par le Nouveau Code pénal

1.1. 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-l 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)

1.2. Crimes et délits contre les bleus

- Escroquerie (art. 313-l et suite)
- Atteintes aux systèmes de traitement automatisé de données (art. 323-l à 323-7 modifiés par la loi 2004-575 du 21 juin 2004).

1.3 Cryptologie

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

2. Infractions de presse (loi 29 juillet 1881, modifiée)

- Provocation aux crimes et délits (art. 23 et 24)
- Apologie des crimes contre l'humanité (art. 24)
- Apologie et provocation au terrorisme (art. 24)
- Provocation à la haine raciale (art. 24)
- « Négationnisme » : contestation des crimes contre l'humanité (art. 24 bis)
- Diffamation (art. 30, 31 et 32)
- Injure (art 33)

3. 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. L 52l-4 modifiée par la loi n°2004.204 du 9 mars 2004, art. 34)
- Contrefaçon de marque (art L 7l6-9 - modifié par la loi n° 2004-204 du 9 mars 2004, art 34 et suivants)

4. Participation à la tenue d'une maison de jeux de hasard (« cyber-casino »)

- Art. 1 de la loi du 12 juillet 1983, modifié par la loi du 16 décembre 1992

Institut Régional Supérieur du Travail Éducatif et Social de Bourgogne

2 Rue du Professeur Marion
21000 DIJON

Annexe n° 3 :

Analyses d'impact relatives à la protection des données personnelles

Fiche d'analyse d'impact des données personnelles

Traitement mis en œuvre par le service (à nommer)	
Date de l'identification des risques	
Date où le responsable de traitement a été informé du risque	
Date de la création de la fiche d'analyse d'impact	
DPD	

Description du traitement des données	- - -
Finalités du traitement	-
Evaluation des risques pour les droits et libertés des personnes concernées	- - - -
Mesures envisagées pour éliminer le ou les risques identifiés	- - - -
Date de l'élimination des risques identifiés à la suite des mesures prises	-
Signatures du responsable de traitement ou du sous-traitent	-

Institut Régional Supérieur du Travail Éducatif et Social de Bourgogne

2 Rue du Professeur Marion
21000 DIJON

Annexe n° 4 :

Notification de violation des données personnelles

Fiche de violation des données personnelles

Traitement mis en œuvre par le service (à nommer)	
Date de l'identification d'une violation des données	
Date de la création de la fiche de violation des données	
Date où le responsable de traitement a été informé de cette violation	
Responsable du traitement	
DPD	

Description du traitement des données	- - -
Finalités du traitement	-
Nature des violations des données personnelles et dimension juridique	- - - -
Mesures prises pour informer les personnes concernées	- - -
Mesures prises pour informer la CNIL	- - -
Violation volontaire et délibérée Ou violation involontaire	-
Un recours a-t-il été demandé par la personne concernée *(Article 79 - Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant)* date à préciser	- -
Signatures du responsable du traitement ou sous-traitant	-

Annexe n°5

Tableaux des suivis réunions d'équipes sur la mise en conformité RGPD

Dates	Equipes concernées	Objets des échanges	Réponses apportées ou travail engagé	Difficultés résiduelles
JANVIER 2023				
31 janvier 2023	DPD	Mise à jour de la charte informatique	Mise à jour de la charte informatique	
21 janvier 2023	Service sélection et admission	Demande de mise à jour des mentions légales sur les documents remis aux candidats et sur site IRTESS	Proposition d'une mention légale du RGPD	
20 janvier 2023	Service sélection et admission	Travail sur les durées de conservation des archives courantes, intermédiaires et définitives	Travail en cours sur certains fichiers et finalisé sur d'autres	Les archives définitives stockées en sous-sol
20 janvier 2023	FFT	Durées de conservation des archives courantes, intermédiaires et définitives	Proposition de durées selon contenus des fichiers et travail	Les archives définitives stockées en sous-sol
17 janvier 2023	Bourgogne FRANCHE COMPTE	Demande de renseignements sur des informations non communiquées par les candidats (NIR)	Nous ne disposons pas des informations et qu'il revient aux candidats de communiquer les informations	
10 janvier 2023	Tous les salariés	Mise à jour de la charte informatique	Travail engagé entre la DPD, la responsable du CERDIM, et le prestataire de service PSI sur les modalités de fonctionnements du système informatique et son développement	La protection des fichiers dans les ordinateurs portables
4 janvier 2023	TISF	Demande de mise à jour du règlement d'admission	Mise à jour du règlement d'admission	