CHARTE INFORMATIQUE ET LIBERTES CFAB

PREAMBULE

Le centre de formation des apprentis du Beaujolais (ci-après « l'établissement ») est un organisme privé de formation portant le projet de favoriser l'insertion sociale des jeunes, développer leur aptitude à l'emploi et permettre l'épanouissement de leur personnalité à la fois en tant que travailleur, citoyen et personne.
Dans le cadre de ses activités, l'établissement est amené à collecter et traiter un certain nombre de données à caractère personnel. L'établissement met également à la disposition des personnels et des apprenants l'ensemble des moyens informatiques nécessaires à l'accomplissement de leurs missions ou de leur formation.
La présente charte a pour objet d'encadrer les opérations menées sur les données personnelles collectées et de définir les conditions d'accès, les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication de l'établissement. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite.
Chaque apprenant et membre du personnel est tenu de respecter la présente charte annexée au règlement intérieur de chacun. Toute violation (imprudence, négligence, malveillance) par les utilisateurs de l'établissement peut donner lieu à l'application des sanctions définies dans le règlement intérieur en fonction de la gravité des faits reprochés et/ou de leurs conséquences en fonction du préjudice subi ou susceptible d'être subi par l'établissement.

ARTICLE 1 – DEFINITIONS

Administrateur informatique : personnel habilité par la direction de l'établissement à effectuer des interventions et des contrôles sur le système d'information pour assurer son fonctionnement normal, qu'il soit salarié de l'établissement ou d'une entreprise extérieure.

Système d'information : Terme générique regroupant le service informatique et les outils numériques et de communication utilisés dans l'établissement.

Intranet : Réseau interne à un établissement permettant de relier du personnel à distance, ou fréquemment à l'extérieur et utilisant le réseau internet.

Extranet : Réseau ouvert aux partenaires de l'établissement et permettant de relier le personnel interne et celui des partenaires.

Données personnelles : Désigne toutes les informations sous quelque forme qu'elles soient se rapportant à une personne physique identifiée ou identifiable, qui sont collectées et traitées sur le système d'information ou sur un support externe.

Personne concernée : désigne l'apprenant, son éventuel responsable légal ou le personnel CFAB.

Utilisateur : toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de l'établissement et à les utiliser : formateurs, apprenants, salariés, bénévoles, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels...

ARTICLE 2 – COLLECTE ET TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

La collecte et le traitement des données personnelles se font en application du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement Général sur la Protection des Données ou « RGPD »), et de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Loi Informatique et Libertés).

2.1 Nature

Les données personnelles collectées ou traitées au sujet de la personne concernée peuvent inclure :

- l'identification générale et les informations de contact : état civil et coordonnées de l'apprenant, du responsable légal, du personnel CFAB ;
- le suivi des activités de formation (notes, bulletins réguliers, relevés d'absences/retards, sanctions…) ;
- la facturation des formations (pour laquelle des données employeur peuvent être collectées et traitées) ;
- les informations financières (numéro de compte bancaire, RIB/IBAN…) ;
- les informations relatives à la santé (protocole relatif aux besoins spécifiques de l'apprenant, mesures médicales d'urgence en cas de pathologie chronique, protocole relatif aux aménagements raisonnables, fiches sanitaires, certificats médicaux…)

Il est essentiel que ces données soient à jour. Pour ce faire, la personne concernée s'engage à communiquer toute modification utile.

2.2 Finalités

Les données sont collectées pour des finalités déterminées et légitimes, nécessaires à l'exécution des missions de formation du CFAB, nécessaires à la sauvegarde des intérêts vitaux de la personne concernée (ou d'une autre personne physique) ou en vertu d'une obligation légale. Elles font l'objet des traitements principaux nécessaires à :

- La gestion de l'inscription, de la prise de poste dans l'établissement ;
- La gestion administrative et comptable ;
- La gestion des activités éducatives et pédagogiques (listes de classes, de groupes, …) ;
- L'utilisation d'outils de travail informatisés (ENT, intranet, tablettes, …) ;
- Le suivi de la formation, y compris lié à des situations particulières (PAI, RQTH, PAP, …)
- L'inscription aux examens ;
- La gestion de la restauration, et des services annexes.

2.3 Destinataires et tiers autorisés

Les données personnelles communiquées sont susceptibles d'être transmises aux destinataires et tiers autorisés suivants :

- l'organisme de gestion de l'établissement, les opérateurs de compétences, les autorités académiques et les collectivités territoriales de rattachement ;
- les services de santé, de secours aux personnes ;
- les organismes publics, les auxiliaires de justice, les officiers ministériels, afin de se conformer à toute loi ou réglementation en vigueur, ou pour répondre à toute demande judiciaire ou administrative.

2.4 Droits et protection

En application du règlement (UE)2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, chapitre III, la personne concernée dispose d'un droit d'accès, de rectification, d'effacement, de limitation et d'opposition au traitement de ses données sous réserve des limitations prévue par la base légale du traitement concerné.
Ces droits peuvent être exercés auprès du responsable du traitement en adressant un email à rgpd@arfa-formation.fr ou un courrier à l'attention de M. AUDARD – Directeur Général du CFAB accompagné de la photocopie d'un titre d'identité comportant la signature de la personne concernée, à l'adresse figurant en pied de page du présent document.
Si la personne concernée estime que ces droits sur ses données ne sont pas respectés, elle peut adresser une réclamation à la CNIL.

ARTICLE 3 – LES REGLES D'UTILISATION DU SYSTEME D'INFORMATION

3.1 L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte ("login" ou identifiant) fourni à l'utilisateur lors de son arrivée dans l'établissement. Un mot de passe temporaire est associé à cet identifiant de connexion (il sera à modifier lors de la première connexion). L'identification de l'utilisateur est obligatoire. Les informations qu'il donne doivent être exactes et actuelles. A défaut, l'ouverture du compte d'accès ne pourra être effective. Les moyens d'authentification sont personnels et confidentiels.

3.2 Les règles d'utilisation et de sécurité

L'utilisateur est responsable de l'usage qu'il fait du réseau. Il assure notamment, à son niveau, la sécurité de ce réseau et s'engage à ne pas apporter volontairement de perturbations à son fonctionnement et à mettre en péril l'intégrité des ressources informatiques.

L'utilisateur s'engage, notamment, à :

- se déconnecter immédiatement après la fin de leur période de travail sur le réseau ou lorsqu'il s'absente ;
- ne pas interrompre le fonctionnement normal du réseau ou des systèmes connectés ;
- ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, saturer les ressources ;
- ne pas introduire des programmes virus, ou contournant la protection des logiciels ;
- ne pas installer de logiciels susceptibles de modifier la configuration des machines sans accord préalable de l'administrateur ;
- ne pas s'attaquer aux systèmes d'information de l'établissement ou de tout autre organisme public ou privé, européen ou étranger, en modifier ou altérer le contenu ;
- ne pas collecter ou tenter de collecter des informations susceptibles d'être utilisées lors de tentatives d'attaques contre des systèmes d'information externes ou internes ;
- ne pas utiliser les ressources informatiques afin de dupliquer, diffuser ou distribuer des logiciels, images, sons et vidéos aux contenus visés par le code pénal ou collectés par des moyens contraires au droit de la propriété intellectuel, sous quelque forme que ce soit ;
- plus généralement, ne pas utiliser les équipements mis à sa disposition à des fins personnelles ou en dehors du cadre strict de ses missions ou de sa formation, sauf autorisation formelle de la Direction ;
- respecter les personnes et l'institution (pas d'atteinte à la vie privée ou au secret de la correspondance, ni d'injures ou de diffamation) ;
- respecter l'ordre public qui condamne le racisme, l'antisémitisme ou l'apologie du crime ;
- respecter le droit d'auteur des œuvres littéraires, musicales, photographiques ou audiovisuel mis en ligne, respecter la propriété intellectuelle pour les logiciels ;

- ne pas porter atteinte à l'intégrité de tout ou partie de ces matériels, à leurs accessoires ou périphériques ;
- ne pas brancher de périphériques (clef USB, smartphone, lecteur MP3, etc…) sur les postes informatiques ;

- ne pas débrancher une prise électrique afin de recharger leurs périphériques (smartphone, lecteur MP3, etc…)

Précisions complémentaires s'agissant des utilisateurs "apprenants" :

Les obligations susvisées s'imposent à l'ensemble des utilisateurs, donc aux apprenants. En complément, il est précisé que :

- Les apprenants travaillent sur le réseau et enregistrent leurs documents dans leur dossier (répertoire) personnel. Ils n'ont accès qu'à leur dossier personnel, et aux documents qui leur sont fournis par leur formateur dans un dossier explicitement prévu à cet effet.
- L'organisation ou la composition des disques durs ou des partitions d'espace disque locales ou distantes ne doit pas être modifiée. Aucune installation ou désinstallation de programme ne doit être effectuée. Aucun enregistrement ou effacement de fichiers n'est autorisé, sauf dans le dossier personnel de l'apprenant.
- L'interface du système (Windows, etc.) ne doit subir aucune modification : icônes, groupe de programme, menus, raccourcis, panneau de configuration, etc.
- L'utilisation d'Internet ne doit se faire que dans le cadre des consignes de recherche données par le formateur. Les contenus écrits ou audiovisuels trouvés sur Internet doivent correspondre strictement à l'objet du travail demandé par le formateur.
- Les apprenants ne doivent pas intervenir sur le matériel (unité centrale, souris, clavier, moniteur, imprimante, etc.). Toute défaillance matérielle doit être immédiatement signalée à un formateur.
- Les salles informatiques doivent être tenues dans un parfait état d'ordre et de propreté. Les matériels utilisés doivent être éteints en fin de séance de travail, sauf consignes particulières. Les documents personnels sont rangés, les chaises remises en place et les papiers usagés mis à la corbeille.
- L'accès aux salles informatiques ou aux postes informatiques en libre-service est interdit sans la présence d'un personnel CFAB. Les jeux y sont formellement interdits.
- Aucun déplacement, aucune permutation d'un quelconque matériel (accessoires, périphériques, etc.) ou d'une partie de celui-ci n'est autorisé. La dégradation, la destruction volontaire ou le vol de tout ou partie d'un matériel sera passible d'une sanction disciplinaire d'exclusion.
- Le compte d'accès comprenant identifiant et mot de passe est strictement personnel. Quiconque détient le mot de passe ou la carte d'accès d'un tiers est considéré en fraude quel qu'en soit le motif. La connaissance accidentelle d'un mot de passe doit être signalée immédiatement au formateur qui demandera à l'administrateur d'en effectuer la réinitialisation.
- Utiliser le réseau pour s'affranchir d'un travail personnel est considéré comme une faute assimilable à un cas de tricherie. Les formateurs ont le droit de consulter les fichiers des élèves même archivés dans leur répertoire personnel.

Utilisation de la messagerie électronique par le personnel :

L'usage privé de la messagerie (envoi et réception de messages) devra gêner le moins possible le trafic normal de messages professionnels, et ce en termes de volume et de taille des messages échangés et de format des pièces jointes.

L'administrateur peut limiter le format, le type et la taille des messages électroniques, y compris les pièces jointes envoyées, notamment par note de service. Les messages non conformes à ces limitations ou comportant un virus ne seront pas distribués.

L'établissement ne garantit pas que le service de messagerie soit exempt de toute interruption, retard, incident de sécurité ou erreur.

L'établissement ne garantit pas les résultats pouvant être obtenus à l'aide de ce service, ni la précision ou la fiabilité des informations acquises par son intermédiaire.

ARTICLE 4 – SERVICES MIS A DISPOSITION

L'établissement met à la disposition de l'utilisateur, dans la mesure de ses capacités techniques, les services suivants :

- les logiciels ou progiciels nécessaires à l'accomplissement de ses missions ou études ;
- l'accès Internet en cas de besoin validé par la Direction, avec possibilité de navigation sur le réseau Internet dans son ensemble ou accès filtré pour gérer l'égalité d'accès aux ressources ;
- l'accès Intranet ou Extranet en cas de besoin validé par la Direction, avec possibilité de navigation sur les réseaux dans leur ensemble ou accès filtré pour gérer l'égalité d'accès aux ressources ;
- l'accès à la messagerie électronique en cas de besoin validé par la Direction ;
- l'accès au site de l'établissement et notamment à ses pages interactives, ainsi qu'à d'autres sites institutionnels ;
- d'un accès au réseau par wifi dont l'accès est validé par la direction.

ARTICLE 5 – ACCES ET CONTRÔLE

Pour assurer le bon fonctionnement du système d'information de l'établissement, il peut être procédé à des contrôles.

5.1 Contrôle global et non nominatif

Des contrôles globaux et non nominatifs seront réalisés sur :

- le nombre de messages échangés ;
- la taille des messages échangés ;
- le format des pièces jointes ;
- les durées de connexion ;
- les sites visités.

L'établissement informe les utilisateurs que les données informatiques concernant l'utilisation de la messagerie et du réseau Internet seront enregistrées et que la durée de conservation de ces données ne pourra excéder six mois.

5.2 Accès et contrôle des messages reçus ou envoyés par l'utilisateur

Un message envoyé ou reçu depuis le poste de travail ou depuis le système de messagerie électronique de l'établissement mis à la disposition de l'utilisateur revêt un caractère professionnel, sauf mention « personnel » ou indication manifeste dans l'objet du message ou dans le nom du répertoire où il pourrait avoir été archivé par son destinataire qui lui conférerait le caractère et la nature d'une correspondance privée protégée par le secret des correspondances.
Dans le cadre de son pouvoir, la direction pourra contrôler le contenu des messages professionnels.
Les utilisateurs ne peuvent avoir accès qu'aux messages qu'ils ont eux-mêmes envoyés ou reçus, sauf autorisation de la direction.

5.3 Accès et contrôle des données enregistrées sur le système d'information

Sauf risque ou évènement particulier, la direction ne pourra ouvrir les fichiers et dossiers identifiés par l'utilisateur comme « personnels », contenus dans le système d'information, qu'en présence de ce dernier ou après l'avoir appelé.
Dans le cadre de son pouvoir, la direction pourra contrôler le contenu des données professionnelles.

Les utilisateurs ne peuvent avoir accès qu'aux données professionnelles qui concernent leur fonction dans l'établissement.

5.4 Rôle de l'administrateur et obligation de confidentialité

L'administrateur informatique pourra avoir accès aux données enregistrées dans le système d'information, même lorsqu'elles ont un caractère personnel, dans les cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par d'autres moyens moins intrusifs.
Cependant l'administrateur informatique est tenu au secret professionnel et à une obligation de confidentialité concernant les données personnelles auxquelles il a accès durant l'exercice de sa mission.
Il ne peut divulguer des informations qu'il aurait été amené à connaître dans le cadre de sa fonction, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique du système d'information ni l'intérêt de l'établissement.

ARTICLE 6 – DISPOSITIONS LEGALES ET REGLEMENTAIRES

En France, des lois et textes réglementaires définissent les droits et obligations des personnes utilisant les moyens informatiques. Les lois les plus importantes sont :

- La loi du 6 janvier 1978 modifiée sur l'informatique et les libertés :
  - Cette loi a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique. Elles définissent les droits des personnes et les obligations des responsables de fichiers.
- La loi du 3 juillet 1985 sur la protection des logiciels :
  - Cette loi protège les droits d'auteurs. Elle interdit en particulier à l'utilisateur d'un logiciel toute reproduction autre que l'établissement d'une copie de sauvegarde.
- La loi du 5 janvier 1988 relative à la fraude informatique :
  - C'est la loi la plus importante et la plus astreignante puisqu'elle définit les peines encourues par les personnes portant atteinte aux systèmes de données.

L'utilisateur s'engage de plus à respecter d'autres dispositions légales et réglementaires en vigueur, comme :

- Celles relatives à la propriété littéraire et artistique, contenues, en particulier, dans le code de la propriété intellectuelle. Le téléchargement de logiciels ou d'œuvres protégées, sans autorisation des ayant-droits engage la seule responsabilité de l'utilisateur. L'administrateur se réserve la possibilité d'effacer du système d'information toute trace de ces logiciels et œuvres.
- Celles relatives à l'Informatique, aux fichiers et aux libertés (loi du 6 janvier 1978).
- Celles relatives à la protection de la vie privée et du droit à l'image d'autrui.

En outre, en application du principe de neutralité commerciale applicable à l'établissement, l'utilisateur s'interdit de faire de la publicité sur des produits et services à caractère commercial, dans le cadre de la diffusion d'informations sur des espaces mis à sa disposition sur le site de l'établissement.
En application du principe de neutralité politique applicable à l'établissement, l'utilisateur s'interdit toute prise de position sur des sujets politiques généraux ne portant pas directement sur les missions de l'établissement.
L'utilisateur s'interdit de produire des contenus à caractère raciste, pornographique, pédophile, injurieux, diffamatoire, incitant à la consommation de substances illicites, à la commission de crimes ou délits, au suicide ou de nature à porter préjudice, de manière générale à l'image de la communauté éducative ou de l'établissement.
L'utilisateur s'interdit, par ailleurs, la consultation ou le téléchargement de documents en provenance de sites illicites, notamment les sites à caractère pédophile ou xénophobe.
Le constat par l'administrateur de manquements à ces obligations par l'utilisateur entraîne son exclusion immédiate des services mis à disposition.
Par ailleurs, l'établissement dénoncera tout acte délictueux aux autorités judiciaires, et ce, sans préjudice de l'application de sanctions.

ARTICLE 7 – RESPONSABILITES ET SANCTIONS

Chaque utilisateur est responsable de l'usage du système informatique mis à sa disposition et s'engage à ne pas effectuer des opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement normal du réseau, sur l'intégrité de l'outil informatique et sur les relations internes et externes de l'établissement.
L'établissement, n'exerçant aucun contrôle éditorial, ne peut être tenu pour responsable du contenu des messages envoyés ou reçus par l'utilisateur.
L'établissement décline toute responsabilité concernant la destruction ou perte de données suite à la connexion de matériel personnel (ordinateur portable ou autre) au réseau de l'établissement quel que soit le moyen (filaire, wifi, autre).

Le personnel d'encadrement est chargé de faire respecter cette charte.

En cas d'anomalie, tout utilisateur doit se rapprocher de l'administrateur informatique qui effectuera le diagnostic de l'anomalie et réparera dès que possible. L'administrateur informatique est habilité à transmettre toute difficulté à la direction de l'établissement dans le respect de son obligation de confidentialité rappelée à l'article 5.4 de la présente charte.

L'utilisateur ne doit en aucun cas entraver l'exercice des fonctions de l'administrateur informatique.

Outre les sanctions pénales ou civiles prévues par les lois, décrets ou textes en vigueur, les utilisateurs encourent en cas de non-respect des dispositions de la présente charte des sanctions disciplinaires prévues par leur règlement intérieur. Il est ici précisé, que dans le cas d'un utilisateur mineur non émancipé, ses responsables légaux répondent civilement des actes de ce dernier.

Je soussigné(e),

NOM : . . . . . PRENOM : . . . . . .
Classe : . . . . . .

déclare, après avoir pris connaissance de la Charte Informatique et Libertés (dont un exemplaire m'a été remis), m'engager à la respecter scrupuleusement.

A ……., le . . . . . / . . . . . / . . . . . .

Signature :