RÈGLEMENT INTÉRIEUR DE L'INSTITUT CATHOLIQUE DE TOULOUSE
APPLICABLE AUX APPRENANTS ET AUX VISITEURS EXTERIEURS AUTORISES

Adopté par le Conseil d'Etablissement de l'ICT le 15 mai 2024

PREAMBULE

L'Institut Catholique de Toulouse (ICT) est un Etablissement d'Enseignement Supérieur Privé d'Intérêt Général (EESPIG) dont le siège social est établi 31, rue de la Fonderie BP 7012 31068 Toulouse Cedex 7. C'est une association Loi 1901 reconnue d'utilité publique par le décret du 22/11/2001 déclarée en Préfecture de la Haute Garonne sous le N° RNA W313006581 - SIRET n° 776 944 100 00010 – Code APE : 8542Z.
L'Institut Catholique de Toulouse est également un organisme de formation continue enregistré sous le numéro de déclaration 73 31 00401 31 auprès de la Préfecture.

L'ICT propose et dispense des formations courtes ou longues en formation initiale ou en formation continue tout au long de la vie, en alternance ou non. Ces formations peuvent se dérouler sur un des 2 campus de l'ICT :

- Le campus de Toulouse, réparti sur 3 sites :
  - 31, rue de la Fonderie 31000 TOULOUSE ;
  - 7-8, Place du Parlement 31000 TOULOUSE ;
  - 22, rue des Fleurs 31000 TOULOUSE.

- Le campus de Bordeaux : 2-8 Allée Marianne Loir 33 800 BORDEAUX.

OBJET ET CHAMP D'APPLICATION DU REGLEMENT

Le présent règlement intérieur a pour objet de définir les règles générales et permanentes en matière d'hygiène et de sécurité et de discipline sur le campus de Toulouse.

Il s'applique à l'ensemble des apprenants inscrits à l'ICT, qu'ils soient :

- Apprenants en formation initiale ;
- Apprenants sous contrat d'apprentissage ou de professionnalisation ;
- Stagiaires de la formation continue ;
- Auditeurs libres.

Ainsi qu'aux visiteurs extérieurs autorisés.

Il définit également les modalités de représentation des apprenants.

Pour les stagiaires en formation continue, conformément à l'article R 6352-1 du code du travail, lorsque la formation se déroule dans une entreprise ou un établissement déjà doté d'un règlement intérieur, les règles d'hygiène et de sécurité applicables aux stagiaires sont celles de ce dernier règlement.
Le règlement intérieur de l'ICT est consultable sur Scolaweb (https://scolaweb.ict-toulouse.fr) et par affichage aux accueils des trois sites.

SECTIONS APPLICABLES A TOUS LES APPRENANTS ET VISITEURS AUTORISES

SECTION 1 : PRINCIPES GENERAUX

1.1. HYGIENE ET SECURITE

La prévention des risques d'accidents et de maladies est impérative et exige de chacun le respect de toutes les prescriptions applicables

en matière d'hygiène et de sécurité en vigueur au sein de l'établissement.
Le Recteur de l'ICT est responsable de la sécurité dans l'enceinte de l'établissement.
Chaque apprenant inscrit à l'ICT ou visiteur autorisé doit veiller à sa sécurité personnelle et à celle des autres en respectant scrupuleusement les consignes générales et particulières de sécurité et d'hygiène en vigueur sur le lieu de formation. En cas de non-respect avéré, des sanctions disciplinaires peuvent être prononcées.

1.1.1. CONSIGNES DE SECURITE

Tout apprenant inscrit à l'ICT ou tout visiteur autorisé présent dans les locaux de l'ICT doit impérativement prendre connaissance et respecter les consignes de sécurité incendie du bâtiment dans lequel il se trouve. Elles sont affichées dans le bâtiment et présentées dans le document « Consignes de sécurité » (en annexe 1) de manière à être connues de tous.
Elles comprennent notamment un plan de localisation des extincteurs et des issues de secours.
Comme tous ~~l~~es membres de la communauté universitaire, tout apprenant inscrit à l'ICT ou tout visiteur autorisé, est tenu d'exécuter sans délai l'ordre d'évacuation des locaux et de respecter les consignes données à cette occasion par le chef d'établissement ou son représentant.
En cas de déclenchement de l'alarme incendie, chacun doit immédiatement évacuer les locaux puis attendre les consignes avant de réintégrer les locaux.

Afin de garantir le libre accès des issues de secours des bâtiments, il est interdit de stationner ou de positionner du mobilier ou du matériel dans les zones de circulation permettant l'évacuation des occupants des locaux de l'ICT. Il est interdit de garer des véhicules dans la cour du 31 rue de la Fonderie sans autorisation.
Les couloirs et les escaliers devront spécialement être laissés libres de tout objet ou mobilier faisant obstacle au passage.
Il est strictement interdit de rendre inutilisable une sortie ou issue de secours réglementaire.
Les installations et équipements de sécurité Incendie (extincteur, systèmes d'alarme...) ont pour but de préserver la vie des personnes en cas de sinistre.

Le non-respect de ces consignes ainsi que toute détérioration volontaire de ces matériels expose le contrevenant concerné à des sanctions disciplinaires et éventuellement pénales pour mise en danger de la vie d'autrui (art. 121-3 du code pénal). Tout déclenchement non justifié est aussi pénalement sanctionné (article 322-14 du code pénal).

L'organisation périodique d'exercice d'évacuation dans les locaux de l'ICT est une obligation règlementaire à laquelle nul membre de la communauté universitaire ne peut se soustraire, sous peine d'encourir des sanctions disciplinaires.
Il appartient à chacun de veiller à chaque instant par son comportement et son activité à la prévention du risque incendie (stockage de papier, utilisation de produits inflammables, d'appareils électriques...) et de signaler tout élément anormal à l'accueil principal de l'ICT (31, rue de la Fonderie, 05 61 36 81 00). Les ventilateurs doivent être débranchés après toute utilisation.

1.1.2. CONSIGNES EN CAS D'ACCIDENT, D'URGENCE MEDICALE OU DE CRISE SANITAIRE

Tout accident ou incident, doit être immédiatement signalé par la victime de l'accident ou toute personne témoin de l'accident à l'accueil principal de l'ICT au 31, rue de la Fonderie (05 61 36 81 00).

Dans le cas d'une crise sanitaire annoncée par le gouvernement, tout apprenant inscrit à l'ICT ou tout visiteur autorisé présent dans les locaux de l'ICT doit impérativement respecter les consignes affichées au sein de l'ICT en conformité avec les directives ministérielles.
Ces règles s'appliquent au sein de tous les espaces de l'ICT (salle de cours, couloirs, locaux

de la vie étudiante, self, espaces de travail partagés, café ICT, bibliothèque.

1.1.3. TABAC, ALCOOL, STUPEFIANTS, OBJETS DANGEREUX INTERDICTION DE FUMER

Conformément au décret n°2006-1386 du 15 novembre 2006 (article R. 3511-1 du code de la santé publique) pris en application de la loi n°31-32 du 10 janvier 1991, tous les locaux des bâtiments de l'ICT sont entièrement non-fumeur. Il est strictement interdit de fumer dans l'enceinte de l'ICT, y compris dans les cours intérieures, les jardins et les porches d'accès.

L'utilisation de la cigarette électronique est également interdite dans l'enceinte de l'ICT.
Cependant, afin de limiter les risques liés à la présence de personnes sur la voie publique, l'ICT a mis en place deux espaces fumeurs extérieurs (situés sur le site de la Fonderie) qui devront impérativement être respectés. Les utilisateurs sont tenus de mettre leurs mégots dans les cendriers prévus à cet effet.
Le non-respect de ces dispositions expose son auteur à des sanctions disciplinaires.

VENTE ET CONSOMMATION D'ALCOOL, ORGANISATION D'EVENEMENTS FESTIFS

Il est interdit aux apprenants de pénétrer ou de séjourner dans l'établissement en état d'ivresse ainsi que d'y introduire des boissons alcoolisées.
L'entrée ou la présence dans l'enceinte de l'établissement d'une personne manifestement en état d'ébriété doit être immédiatement signalée à l'accueil du site qui en réfèrera à son responsable.
La consommation et la vente d'alcool sont interdites dans l'enceinte de l'ICT.
Le non-respect de ces dispositions expose son auteur à des sanctions disciplinaires.
Une dérogation peut être accordée à titre exceptionnel par le Recteur de l'ICT. Tout organisateur d'un évènement festif pour les apprenants de l'ICT au sein de l'ICT doit au préalable transmettre une demande d'autorisation au Recteur.

INTRODUCTION DE SUBSTANCES DANGEREUSES

Il est interdit d'introduire sur les sites de l'ICT toute substance (notamment stupéfiants), tout matériel ou instrument dangereux (notamment armes), illicite, nuisible à la santé ou contraire aux impératifs de salubrité ou d'ordre public, sauf autorisation expresse des autorités compétentes.

De tels faits donneront lieu à l'engagement d'une procédure disciplinaire indépendante de la mise en œuvre d'éventuelles poursuites pénales.

1.1.4. COMPORTEMENT ET RESPECT DES PERSONNES

TENUE ET COMPORTEMENT

Lorsqu'ils se présentent en cours ou en examens, et lorsqu'ils fréquentent les espaces communs (self, espaces de travail partagés, café ICT, bibliothèque, foyer, etc.), les apprenants doivent adopter une tenue vestimentaire décente et un comportement respectueux des personnes et des biens.

Les apprenants doivent notamment se conformer à la loi n° 2010-1192 du 11 octobre 2010 interdisant la dissimulation du visage dans l'espace public.

Lors des examens, le port de tenues vestimentaires ne doit pas rendre impossible ou difficile l'identification des apprenants ou être susceptible d'engendrer un doute sur cette identification et ne doit pas aller à l'encontre des nécessités liées à l'organisation et au bon déroulement des épreuves.

Les règles élémentaires de civisme, politesse, respect, d'hygiène et de sécurité envers chacun, à l'intérieur ou aux abords de l'ICT sont l'affaire de chacun pour le bien-être de tous :

- Un niveau sonore raisonnable doit être respecté devant l'ICT pour des questions de bon voisinage. Il en est de même à l'intérieur de l'ICT par respect pour les différents membres de la communauté universitaire ;

- Pour raison de sécurité des personnes (accident de la circulation, plan Vigipirate…), tout comme de civisme (notamment envers le voisinage et les personnes circulant dans l'espace public), il est demandé de ne pas rester en groupe devant l'entrée de l'ICT, de ne pas y gêner le passage des personnes et des véhicules, de ne pas laisser de détritus sur la voie publique (notamment gobelet, mégots...) et d'utiliser les équipements dédiés installés à l'intérieur de l'ICT ou sur la voie publique ;

- Les apprenants doivent respecter les heures du début et de fin des cours.
L'ICT se réserve le droit de modifier les horaires de cours en fonction des nécessités de service. Les apprenants doivent alors s'y conformer.
En cas d'absence ou de retard, il est préférable pour l'apprenant d'en avertir l'établissement dans les plus brefs délais en contactant le secrétariat de la faculté, de l'école ou de l'institut dont il dépend ;

- L'usage du téléphone portable pendant les cours et toute autre activité universitaire est strictement interdit (sauf si l'enseignant l'autorise dans un cadre précis ou en cas de force majeure) ;

- Sauf dérogation expresse, il est formellement interdit d'enregistrer ou de filmer les sessions de formation.

DISCRIMINATIONS

En vertu de l'article 225-1 du code pénal, « constitue une discrimination toute distinction opérée entre les personnes physiques sur le fondement de leur origine, de leur sexe, de leur situation de famille, de leur grossesse, de leur apparence physique, de la particulière vulnérabilité résultant de leur situation économique, apparente ou connue de son auteur, de leur patronyme, de leur lieu de résidence, de leur état de santé, de leur perte d'autonomie, de leur handicap, de leurs caractéristiques génétiques, de leurs mœurs, de leur orientation sexuelle, de leur identité de genre, de leur âge, de leurs opinions politiques, de leurs activités syndicales, de leur qualité de lanceur d'alerte, de facilitateur ou de personne en lien avec un lanceur d'alerte au sens, respectivement, du I de l'article 6 et des 1° et 2° de l'article 6-1 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, de leur capacité à s'exprimer dans une langue autre que le français, de leur appartenance ou de leur non-appartenance, vraie ou supposée, à une ethnie, une Nation, une prétendue race ou une religion déterminée.

Constitue également une discrimination toute distinction opérée entre les personnes morales sur le fondement de l'origine, du sexe, de la situation de famille, de la grossesse, de l'apparence physique, de la particulière vulnérabilité résultant de la situation économique, apparente ou connue de son auteur, du patronyme, du lieu de résidence, de l'état de santé, de la perte d'autonomie, du handicap, des caractéristiques génétiques, des mœurs, de l'orientation sexuelle, de l'identité de genre, de l'âge, des opinions politiques, des activités syndicales, de la qualité de lanceur d'alerte, de facilitateur ou de personne en lien avec un lanceur d'alerte, au sens, respectivement, du I. de l'article 6 et des 1° et 2° de l'article 6-1 de la loi n° 2016-1691 du 9 décembre 2016 précitée, de la capacité à s'exprimer dans une langue autre que le français, de l'appartenance ou de la non-appartenance, vraie ou supposée, à une ethnie, une Nation, une prétendue race ou une religion déterminée des membres ou de certains membres de ces personnes morales. »

De tels faits donneront lieu à l'engagement d'une procédure disciplinaire indépendante de la mise en œuvre d'éventuelles poursuites pénales.

BIZUTAGE ET HARCELEMENT MORAL, VIOLENCES SEXISTES ET SEXUELLES

Le bizutage porte atteinte à la dignité d'autrui. Conformément à l'article 225-16-1 du Code pénal, il constitue un délit et est défini comme suit : *« Hors les cas de violences, de menaces ou*

d'atteintes sexuelles, le fait pour une personne d'amener autrui, contre son gré ou non, à subir ou à commettre des actes humiliants ou dégradants ou à consommer de l'alcool de manière excessive, lors de manifestations ou de réunions liées aux milieux scolaire et socio-éducatif est puni de six mois d'emprisonnement et de 7 500 euros d'amende ».
Les peines sont majorées en cas de particulière vulnérabilité de la victime.

Le bizutage constitue également une faute de nature disciplinaire pouvant entraîner une sanction.

Toute forme de harcèlement moral au sens de l'article 222-33-2 du code pénal (« le fait de harceler autrui par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel ») est interdite et expose son auteur à des sanctions disciplinaires et pénales.

Les violences sexistes et sexuelles recouvrent l'ensemble des situations dans lesquelles une personne impose à autrui un ou des comportements, un ou des propos (oraux ou écrits) à caractère sexiste ou sexuel.
Elles peuvent prendre différentes formes : outrage sexiste, injure, harcèlement sexuel, agression sexuelle, viol…

Ces violences portent atteinte aux droits fondamentaux, et notamment à l'intégrité physique et psychologique des personnes. Elles sont interdites par la loi et punies pénalement.

Toute personne victime ou témoin d'une situation de bizutage, de harcèlement moral ou de violence sexiste ou sexuelle peut en faire le signalement auprès du Recteur ou auprès de la cellule d'écoute psychologique de l'ICT ou auprès du service de la vie étudiante.
Avec l'accord du témoin ou de la victime, la cellule d'écoute psychologique ou le service de la vie étudiante peut transmettre le signalement au Recteur de l'ICT pour assurer le traitement disciplinaire de la situation.

Le Recteur ou le Vice-Recteur à la vie étudiante et au développement académique peut alors décider :
- de déclencher une enquête interne ;
- de mettre en place des mesures conservatoires (comme l'interdiction provisoire d'accéder aux campus de l'ICT) ;
- d'engager une procédure disciplinaire pouvant aboutir à l'exclusion définitive des campus de l'ICT et de tout établissement d'enseignement supérieur public avec lequel l'ICT est en partenariat.
- de saisir en fonction de la situation le Procureur de la République (article 40 du code de procédure pénale).

1.2. COMPORTEMENT ET RESPECT DE L'ENVIRONNEMENT DES LOCAUX ET DU MATERIEL

1.2.1. REGLES GENERALES

Les locaux, y compris les espaces communs, les espaces verts, et les abords de l'ICT, le mobilier et le matériel de toute nature constituent le cadre de vie collective et de travail de tous et doivent être respectés. Il convient donc d'avoir un comportement responsable et de veiller à les conserver en bon état et de maintenir leur propreté.

L'introduction d'animaux de compagnie dans l'enceinte des sites de l'ICT est interdite, à l'exception des chiens-guides tenus en laisse accompagnant les personnes en situation de handicap, les agents de sécurité ou encore leur formateur ou famille d'accueil.

La dégradation volontaire des locaux dans leur acceptation large, ou du mobilier, du matériel pédagogique mis à disposition par l'ICT, en particulier du matériel documentaire, informatique et audiovisuel est passible de sanctions disciplinaires pouvant aller jusqu'à l'exclusion définitive.

De plus, le fait de tracer des inscriptions, des signes ou des dessins, sans autorisation

préalable, sur les façades, les véhicules, les voies publiques ou le mobilier d'autrui est un délit puni par la loi qui expose le contrevenant à des poursuites judiciaires pouvant conduire à une amende de 3 750 euros et une peine de travail d'intérêt général.

1.2.2. L'ENVIRONNEMENT PEDAGOGIQUE

Chacun doit prendre connaissance et se conformer aux règlements d'utilisation des locaux en vigueur concernant en particulier les salles informatiques, les espaces de travail partagés et la bibliothèque universitaire.

En cas d'utilisation autorisée ou de salle en libre accès, les salles doivent être remises en état si les tables et/ou chaises sont déplacées.
Aucun matériel ne doit être déplacé dans une autre salle sans autorisation.

Les apprenants doivent en particulier :

- Se conformer aux règlements d'utilisation des locaux en vigueur : salles de cours, amphithéâtres, salles informatiques, espaces communs, espaces de travail partagés, espace muséographique et bibliothèque universitaire ;
- Veiller à maintenir la propreté des locaux et des abords de l'ICT.
  Pour des raisons d'hygiène, il est interdit de consommer de la nourriture ou des boissons dans les espaces listés ci-dessus. Seules les salles dédiées à la restauration doivent être utilisées à cet effet (self ou espace Café de l'ICT sur le site Fonderie ou salle Saint Dominique sur le site Parlement). Les déchets alimentaires doivent être déposés dans les poubelles prévues à cet effet et non pas dans les corbeilles à papier des bureaux et salles de cours ;
- Prendre soin du mobilier et du matériel pédagogique qui leur est confié pendant leur formation : les apprenants sont tenus de les utiliser conformément à leur objet. L'utilisation à d'autres fins est interdite. A la fin de la formation, l'apprenant est tenu de restituer tout matériel et document pédagogique en sa possession appartenant à l'ICT ;
- Respecter la législation sur les droits d'auteurs et n'utiliser la documentation pédagogique remise au cours de la formation que pour leur usage personnel.

<u>Charte informatique</u>
Lors de l'inscription à l'ICT, chaque apprenant prend connaissance de la charte informatique en annexe 2 et s'engage à en respecter les dispositions.

Le non-respect de ses clauses pourra donner lieu à la suppression de l'accès aux services, à des sanctions disciplinaires ou à des sanctions pénales en cas d'infraction aux lois en vigueur.

1.2.3. LA RESTAURATION

Les apprenants peuvent prendre leurs repas uniquement dans les lieux dédiés à cet effet :

- Self (site Fonderie) : les apprenants ont accès au self pendant toute la durée de la formation suivie, aux horaires affichés.

La carte étudiant ou la carte étudiant des métiers est obligatoire pour bénéficier de la participation de l'ICT au prix du repas. Le rechargement de la carte s'effectue à la caisse avec une somme minimum fixée par le responsable du self. Le pain, les condiments, les couverts, les plateaux, les gobelets ainsi que l'utilisation du micro-ondes sont réservés à l'usage exclusif des clients du self. Il est formellement interdit de porter de la nourriture de l'extérieur pour la consommer dans l'enceinte du self.

- Café ICT (site de la Fonderie) : les apprenants ont la possibilité d'y prendre leurs repas ou des collations. Il peut s'agir de denrées achetées dans les distributeurs qui s'y trouvent ou de nourriture apportée de l'extérieur. Les déchets

doivent être jetés dans les poubelles prévues à cet effet.

- Salle Saint Dominique (site du Parlement) : les apprenants ont également la possibilité d'y prendre leurs repas ou des collations. Il peut s'agir de denrées apportées de l'extérieur. Les déchets doivent être jetés dans les poubelles prévues à cet effet.

RAPPEL : Pour des raisons d'hygiène, il est interdit de prendre ses repas dans les salles de cours, les amphithéâtres, la bibliothèque universitaire, les espaces de coworking, l'espace muséographique... et de jeter les déchets alimentaires, canettes, gobelets dans les corbeilles à papier. Il est demandé d'utiliser les poubelles prévues à cet effet et de pratiquer le tri sélectif en utilisant les dispositifs mis en place dans ce but au sein de l'ICT afin de permettre le recyclage et la valorisation des déchets.

De plus, il est interdit de jeter les déchets sur la voie publique devant l'ICT.

1.2.4. LE PARKING

Dans l'enceinte de l'ICT, les deux roues devront être garés dans les emplacements prévus à cet effet situé uniquement devant l'espace muséographique au 31, rue de la Fonderie et dans la cour au 8 place du Parlement ou, le cas échéant, tout autre lieu communiqué par la Direction de l'ICT. La cour du bâtiment de la recherche est interdite au public.

1.2.5. RESPECT DE L'ENVIRONNEMENT ET DEVELOPPEMENT DURABLE

Dans un souci de respect de l'environnement, chacun doit contribuer activement aux économies d'énergies, de fluides et de consommables, que ce soit en matière de reproduction de documents, de chauffage ou encore d'éclairage (fermer les fenêtres des salles de classe après aération, ne pas bloquer en position ouverte les portes d'accès des bâtiments vers l'extérieur, éteindre la lumière en quittant une pièce…), s'assurer de bien fermer les robinets non-automatiques.

1.3 RESPONSABILITE DE L'ICT EN CAS DE VOL OU ENDOMMAGEMENT DE BIENS PERSONNELS DES APPRENANTS

L'ICT décline toute responsabilité en cas de perte, vol ou détérioration des objets personnels de toute nature, déposés par l'apprenant dans son enceinte (salle de cours, amphithéâtre, locaux administratifs, parc de stationnement, cour, toilettes…).

SECTION 2 : REGLES SPECIFIQUES CONCERNANT LES LOCAUX

2.1. ACCES AUX SITES ET LOCAUX

2.1.1 RESPECT DES HEURES D'OUVERTURE DE L'ICT

L'accès aux différents sites de l'ICT et aux différents locaux qu'ils comportent est strictement réservé aux apprenants, aux personnels et aux autres visiteurs dûment autorisés.
Il est possible uniquement pendant les périodes et les heures d'ouverture de l'ICT.
Ces dernières sont déterminées par le Recteur et affichées à l'accueil de chaque site.
En dehors de ces plages horaires, l'accès aux différents sites de l'ICT est interdit et les apprenants ne sont pas autorisés à rester dans les locaux après la fermeture des sites.

Des horaires particuliers peuvent être décidés pour certains bâtiments et impliquent la mise en place de mesures de sécurité adaptées.

Les apprenants ne sont également pas autorisés à rester dans les salles de cours en dehors des heures de présence de l'enseignant.
Un apprenant ne peut se faire remettre les clés d'une salle sans l'autorisation de l'enseignant responsable ou du secrétariat de la faculté, de l'école ou de l'institut auquel il appartient.

2.1.2 VIDEOPROTECTION ET CONTROLE D'ACCES

Les sites d'enseignement de l'ICT sont placés sous vidéoprotection et contrôle d'accès.
Conformément à la loi n°78-17 du 06 janviers 1978 relative à l'informatique, aux fichiers et aux libertés :

- Les images enregistrées ne sont visualisées que par les personnes dûment autorisées. Ces images enregistrées sont conservées 30 jours maximum ;
- Toute personne intéressée peut demander à accéder aux enregistrements (vidéoprotection, contrôle d'accès) qui le concernent ou vérifier la destruction dans les délais prévus. Cet accès est un droit. Un refus peut être opposé pour un motif tenant au droit des tiers.

Tout apprenant inscrit à l'ICT ou tout visiteur doit se soumettre au dispositif de contrôle d'accès aux bâtiments.

L'accès aux 3 sites de l'ICT du campus de Toulouse se fait grâce à :
- la carte étudiant ou carte étudiant des métiers, délivrée au moment de l'inscription par les secrétariats des formations ; il n'en sera pas délivré de nouvelle en cours d'année, sauf en cas de perte ou de vol, et uniquement sur présentation d'un justificatif officiel (déclaration de perte ou de vol), et contre paiement de 30€ ;
- un badge provisoire remis au visiteur à l'accueil d'un des 3 sites du campus en échange d'une pièce d'identité.

L'accessibilité pour les personnes qui présentent un handicap est détaillée dans la politique d'inclusion et d'accessibilité en annexe 3.

2.1.3 PLAN VIGIPIRATE ET REGLES DE SURETE

La sécurité est l'affaire de tous. Il est donc important d'adopter une démarche de veille, de prévention, de protection et de sécurité.
Le logo indiquant le niveau du plan Vigipirate est affiché à l'entrée des sites de l'ICT.

En fonction du niveau du plan Vigipirate déclenché par le Gouvernement, l'accès aux locaux peut être renforcé pour des raisons liées à la sûreté et à l'ordre public : filtrage des entrées, contrôle visuel des sacs par les agents de sécurité.
Le refus de se soumettre à ces contrôles peut justifier l'interdiction d'accéder aux sites de l'ICT.

Les attitudes ou situations inhabituelles doivent être signalées à l'accueil principal, 31 rue de la Fonderie (05 61 36 81 00) :
- véhicule suspect : stationnement prolongé, comportement des occupants, moteur tournant ;
- attitude laissant supposer un repérage : allées et venues, observations prolongées.
En cas d'alerte, les apprenants devront respecter scrupuleusement les consignes données d'évacuation ou de confinement, par l'établissement ou les forces de l'ordre.

2.2. MISE A DISPOSITION DES LOCAUX

La mise à disposition de locaux à titre permanent au bénéfice d'associations ayant leur activité au sein de l'établissement est décidée par le Recteur de l'ICT ou son représentant. Ce point est traité dans la section 3 paragraphe 2 Liberté d'association.

La mise à disposition occasionnelle de locaux relevant de l'ICT, à quelque titre que ce soit, au bénéfice de manifestations ou d'activités quelconques, et à la demande d'organisateurs intérieurs comme extérieurs à l'ICT, nécessite la délivrance d'une autorisation écrite du Recteur de l'ICT ou de son représentant ou bien la passation d'une convention. Dans tous les cas, les bénéficiaires de l'autorisation ou de la

convention doivent veiller au respect de leurs obligations réglementaires (déclaration de la manifestation en préfecture, assurance responsabilité civile, éventuellement déclaration d'ouverture de débit de boissons temporaire à la mairie) et des relatives à l'hygiène et à la sécurité, notamment en matière de lutte contre l'incendie. Ils s'engagent à transmettre les justificatifs correspondants à leurs obligations à l'ICT.
En cas de non-transmission des documents, l'ICT se réserve le droit de refuser la mise à disposition de ses locaux.
Ce point est complété dans la section 3 paragraphe 3 Liberté de réunion.

SECTION 3 : DROIT ET LIBERTES DES USAGERS

3.1. AFFICHAGE ET DISTRIBUTION DES TRACTS (LIBERTÉ D'INFORMATION ET D'EXPRESSION)

Les apprenants de l'ICT disposent de la liberté d'information et d'expression à l'égard des problèmes politiques, économiques, sociaux et culturels, et l'exercent à titre individuel et collectif (article L811-1 du Code de l'Education).
La distribution et I 'affichage de tracts, avis et communiqués est libre sous conditions :

- Tout document diffusé doit comporter la signature de l'auteur et l'identification de l'imprimeur. Le ou les auteurs assument l'entière responsabilité du contenu des affiches et de leur affichage ;
- La distribution de tracts, avis et communiqués par toute personne étrangère à l'ICT doit faire l'objet de l'autorisation préalable du Recteur de l'ICT ;
- L'ICT met à disposition des panneaux. En dehors des emplacements réservés, tout affichage, de quelque nature qu'il soit, est interdit et peut entraîner des sanctions disciplinaires contre son auteur.

Le personnel de l'ICT est habilité à éliminer tout affichage non conforme à la réglementation en vigueur.

L'exercice de la liberté d'expression ne doit pas :

- Être susceptible d'entraîner de troubles à l'ordre public ;
- Porter atteinte au respect des personnes et à l'image de l'ICT ;
- Porter atteinte au respect de l'environnement ;
- Porter atteinte au fonctionnement et au caractère propre de l'ICT.

3.2 LIBERTE D'ASSOCIATION

Les associations universitaires à caractère scientifique, social, sportif et culturel ne peuvent fixer leur siège à l'ICT que sur autorisation expresse du Recteur de l'ICT. La demande d'autorisation doit être préalable et accompagnée des statuts de l'association en vigueur au moment du dépôt de la demande. Seules les associations dont la majorité des membres du bureau est inscrit en formation initiale ou dans le cadre d'un contrat d'apprentissage à l'ICT sont autorisées à déposer une telle demande. Toute modification ultérieure de ceux-ci devra être communiquée au Recteur de l'ICT.

Les associations étudiantes qui ont leur siège à l'ICT s'engagent à transmettre au Recteur par l'intermédiaire du service de la vie étudiante dans les plus brefs délais un justificatif d'existence légal de l'association (extrait du JOAFE ou récépissé de la déclaration au greffe des associations), ainsi qu'une attestation d'assurance en responsabilité civile pour l'année universitaire en cours ainsi que les coordonnées de leur représentant légal.
Elles s'engagent également à communiquer chaque année au Recteur de l'ICT un rapport d'activité. Cf. annexe 5.

3.3 LIBERTE DE REUNION

Aucune manifestation ou réunion hors du cadre des fonctions de l'ICT ne peut se tenir ou être organisée au sein des locaux de l'ICT sans autorisation préalable du Rectorat de l'ICT et à la condition expresse de veiller à la mise en œuvre des mesures obligatoires de sécurité. Il

en va de même lorsque des apprenants souhaitent inviter dans les enceintes ou locaux de l'établissement des personnes extérieures, sans lien avec l'activité de l'ICT.
Il ne doit exister aucune confusion possible entre l'université et les organisateurs des manifestations qui restent responsables du contenu des interventions. Il incombe au Recteur de l'ICT, en vue de donner ou de refuser son « accord préalable » à la mise à disposition d'une salle ou d'un site de l'ICT, de prendre toutes mesures nécessaires pour à la fois veiller au respect des libertés dans l'établissement, assurer l'indépendance de l'ICT de toute emprise politique ou idéologique et maintenir l'ordre dans ses locaux.

SECTION 4 : DISPOSITIONS DISCIPLINAIRES

Le pouvoir disciplinaire à l'égard des apprenants est exercé par le Vice-Recteur à la Vie étudiante et au développement académique sur délégation du Recteur et éventuellement par le conseil de discipline en formation initiale, la commission de discipline en formation continue.
Ces instances se composent du Vice-Recteur, du Doyen de la faculté ou Directeur de l'école ou de l'institut ou son représentant, du Directeur des études dont dépend l'apprenant, ainsi que d'un représentant apprenant.

En vertu des articles R811-10 et suivants du code de l'éducation, donne lieu à procédure disciplinaire :

- Toute fraude ou tentative de fraude commise à l'occasion d'une épreuve de contrôle des connaissances et des compétences que ce soit dans le cadre d'un contrôle continu ou d'un examen final ;
- Toute fraude ou tentative de fraude à l'inscription ;
- Toutes productions qui ne respectent pas le code de la propriété intellectuelle (annexe 4) ;
- Tout fait de nature à porter atteinte à l'ordre ou au bon fonctionnement ou à la réputation de l'ICT, tout manquement au présent règlement intérieur et à ses annexes ;
- Tout manquement aux règlements des études ou charte des examens de la faculté, de l'école ou de l'institut dont dépend l'apprenant.

Les sanctions disciplinaires applicables aux contrevenants sont proportionnelles à la gravité de la faute commise et sont les suivantes :
- l'avertissement ;
- le blâme ;
- l'exclusion temporaire pour une durée maximum de cinq ans ou l'exclusion définitive de l'ICT ;
- l'exclusion temporaire pour une durée maximum de cinq ans ou l'exclusion définitive de tout établissement public d'enseignement supérieur (décision portée par le Rectorat d'Académie ou par l'Université publique délivrant le diplôme).

Les amendes ou autres sanctions pécuniaires sont interdites.

En cas de fraude ou de tentative de fraude, la sanction encourue peut, selon le cas, conduire à l'annulation de l'inscription ou la nullité de l'épreuve au cours de laquelle s'est produite la fraude ou la tentative de fraude.

Tout fait de nature à déclencher une procédure disciplinaire doit être porté par écrit, avec ses pièces justificatives à l'appui au Doyen de la faculté ou Directeur de l'école ou de l'institut.

Le Doyen ou le Directeur informe le Vice-Recteur à la vie étudiante et au développement académique de l'ICT des faits reprochés à l'apprenant.

En fonction de la gravité des faits reprochés et de la sanction envisagée, le Vice-Recteur, fait appel ou non au conseil de discipline ou à la commission de discipline pour étude du dossier.

Le Vice-Recteur informe l'apprenant par écrit des griefs retenus contre lui et de la possibilité

de consulter son dossier. Il lui indique également les sanctions encourues.

Si l'instruction confirme les faits reprochés, et en fonction de leur gravité, l'apprenant est convoqué par le Vice-Recteur à la vie étudiante et au développement académique ou par son représentant, par mail et par lettre recommandée avec accusé de réception ou remise à l'intéressé contre décharge, au moins quinze jours avant la date fixée, à un conseil de discipline ou une commission de discipline. Il indique l'objet de la convocation, la date, l'heure et le lieu de l'entretien ainsi que la possibilité de se faire accompagner par la personne de son choix.

Au cours du conseil de discipline ou de la commission de discipline, le motif de la sanction envisagée est rappelé à l'apprenant. Celui-ci a alors la possibilité de donner toute explication ou justification des faits qui lui sont reprochés.

Lorsqu'une mesure conservatoire d'exclusion temporaire à effet immédiat est prise, aucune sanction définitive ne peut être prise sans que l'apprenant n'ait été au préalable informé des griefs retenus contre lui et ait été convoqué à un conseil de discipline ou une commission de discipline.
L'absence de l'apprenant à son conseil de discipline n'est pas un motif de report ou d'annulation de la session disciplinaire, hors cas de force majeure.

Le Conseil de discipline ou la commission de discipline émet un avis après avoir entendu l'apprenant.

Le Vice-Recteur à la vie étudiante et au développement académique, après consultation du conseil de discipline ou de la commission de discipline, rend sa décision et en informe l'apprenant.

En cas de sanction, celle-ci ne peut intervenir moins d'un jour franc ni plus de 15 jours après l'entretien ou l'avis du Conseil de discipline.

Elle fait l'objet d'une notification écrite et motivée à l'apprenant sous forme de lettre recommandée avec accusé de réception ou remise en mains propres contre décharge.

Par ailleurs, en cas de sanction à l'encontre d'un stagiaire, la direction de l'ICT en informe :

- L'employeur du salarié stagiaire ou l'administration de l'agent stagiaire lorsque la formation se réalise sur commande de l'employeur ou de l'administration ;
- Le financeur de l'action de formation.

La décision peut faire l'objet d'un recours auprès du Recteur de l'ICT dans un délai de 15 jours à compter de la notification de la décision.

Les dispositions disciplinaires pour les apprenants inscrits dans des formations sous convention avec une université publique relèvent d'un régime spécifique précisé dans le corps du règlement des études ou dans son annexe.

Les dispositions disciplinaires pour les apprenants des facultés ecclésiastiques relèvent d'un régime spécifique précisé dans les statuts des facultés ou dans les statuts canoniques de l'ICT.

SECTIONS APPLICABLES SPECIFIQUEMENT AUX STAGIAIRES DE LA FORMATION CONTINUE ET ETUDIANTS SOUS CONTRAT D'APPRENTISSAGE ET DE PROFESSIONNALISATION

L'ensemble des dispositions des précédentes sections de ce règlement intérieur s'appliquent aux stagiaires de la formation continue et étudiants sous contrat d'apprentissage et de professionnalisation.
Mais certaines spécificités, indépendantes des rubriques présentées ci-dessus, demeurent et sont présentées dans cette section.
Le règlement intérieur est établi conformément aux dispositions des articles L.6352-3 et L.6352-4 et R.6352-1 à R.6352-15 du Code du travail. Toutefois, conformément à l'article R 6352-1 du

Code du travail, lorsque l'action de formation se déroule dans une entreprise ou un établissement déjà doté d'un règlement intérieur, les mesures de santé et de sécurité applicables aux stagiaires sont celles définies dans ce dernier règlement.
Chaque stagiaire est considéré comme ayant accepté les termes du présent règlement durant toute la durée de l'action de formation suivie et accepte que des mesures soient prises à son égard en cas d'inobservation de ce dernier.

SECTION 5 : ORGANISATION DE LA FORMATION

5.1. HORAIRES DE FORMATION

Le stagiaire doit se conformer aux horaires fixés et communiqués au préalable par la direction soit par voie d'affichage, soit à l'occasion de la remise du programme de l'action de formation ou dans l'espace Scolaweb de l'ICT. Le non-respect de ces horaires peut entraîner des sanctions disciplinaires.

5.1.1. ABSENCES, RETARDS OU DEPARTS ANTICIPES

En cas d'absence, de retard ou de départ anticipé, le stagiaire doit avertir le formateur ou le secrétariat de l'ICT chargé de l'action de formation et se justifier auprès d'eux. Par ailleurs, le stagiaire n'est pas autorisé à s'absenter pendant les heures de formation, sauf circonstances exceptionnelles précisées par la direction de l'ICT ou son représentant.
Conformément à l'article R6341-45 du Code du Travail, le stagiaire dont la rémunération est prise en charge par les pouvoirs publics s'expose à une retenue sur sa rémunération de stage proportionnelle à la durée de l'absence.
Lorsque le stagiaire est un salarié en formation dans le cadre du plan de formation, la direction de l'ICT informera préalablement l'entreprise de ces absences. Tout événement non justifié par des circonstances particulières constitue une faute passible de sanctions disciplinaires.

5.1.2. FORMALISME ATTACHE AU SUIVI DE LA FORMATION

Toute demande de rémunération ou de prise en charge des frais liés à la formation, attestation d'inscription ou d'entrée en formation devra être remise dans les meilleurs délais aux services concernés.
Le stagiaire est tenu de remplir ou signer obligatoirement et régulièrement, au fur et à mesure du déroulement de l'action, la feuille d'émargement. Il peut lui être demandé de réaliser un bilan de la formation. A l'issue de l'action de formation, la direction de l'ICT remettra une attestation de fin de formation et une attestation de présence à l'action de formation à transmettre, selon le cas, à son employeur ou à l'organisme financeur de l'action.

5.1.3. CONSIGNES EN CAS D'ACCIDENT

Tout accident ou incident survenu à l'occasion ou en cours de formation doit être immédiatement déclaré à la direction de l'ICT par l'apprenant ou par les personnes témoins de l'accident. Conformément à l'article R 6342-3 du Code du Travail, l'accident survenu à l'apprenant pendant qu'il se trouve sur le lieu de formation ou pendant qu'il s'y rend ou en revient, fait l'objet d'une déclaration par la direction de l'ICT auprès de la caisse de sécurité sociale.

SECTION 6 : REPRESENTATION DES STAGIAIRES

6.1. ORGANISATION DES ELECTIONS

Lorsqu'une action de formation suivie par le stagiaire en formation continue a une durée supérieure à 500 heures, il est procédé simultanément à l'élection d'un délégué titulaire et d'un délégué suppléant en scrutin uninominal à deux tours. Tous les stagiaires sont électeurs et éligibles. L'ICT organise le scrutin qui a lieu pendant les heures de formation, au plus tôt 20 heures, au plus tard 40 heures après le début du stage.

En cas d'impossibilité de désigner les représentants des stagiaires, l'ICT dresse un procès-verbal de carence qu'il transmet au préfet de région territorialement compétent. La direction de l'ICT a la charge de l'organisation du scrutin. Elle en assure le bon déroulement.

6.2. DUREE DU MANDAT DES DELEGUES DES STAGIAIRES

Les délégués sont élus pour la durée de l'action de formation. Leurs fonctions prennent fin lorsqu'ils cessent, pour quelque cause que ce soit, de participer à la formation. Si le délégué titulaire et le délégué suppléant ont cessé leurs fonctions avant la fin de la session de formation, il est procédé à une nouvelle élection dans les conditions prévues aux articles R.6352-9 à R.6352-12 du Code du Travail.

6.3. ROLE DES DELEGUES DES STAGIAIRES

Les délégués des stagiaires font toute suggestion pour améliorer le déroulement des actions de formation et les conditions de vie des stagiaires au sein de l'ICT. Ils présentent toutes les réclamations individuelles ou collectives relatives à ces matières, aux conditions d'hygiène et de sécurité et à l'application du règlement intérieur. Ils ont qualité pour faire connaître au conseil de perfectionnement, lorsqu'il est prévu, les observations des stagiaires sur les questions relevant de la compétence de ce conseil.

ENTREE EN VIGUEUR ET MODIFICATION DU PRESENT REGLEMENT INTERIEUR

Le présent règlement intérieur a été adopté en conseil d'établissement le……et entrera en vigueur à compter du 01/09/2024.

La modification du présent règlement peut être à l'initiative du vice-rectorat à la vie étudiante et au développement académique, des doyens et directeurs, du service qualité et conformité. Pour être adoptée, elle doit être présentée au Conseil d'établissement. L'approbation de la majorité au moins des membres est nécessaire.

Toulouse, le : 19 juin 2024

Professeur François MOOG
Recteur de l'Institut Catholique de Toulouse

ANNEXES

Annexe 1 : Consignes de sécurité

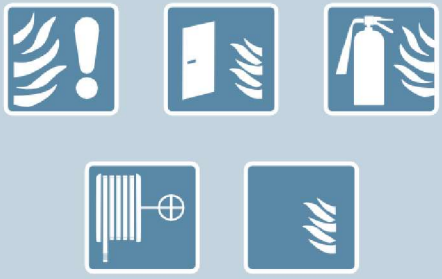
Consignes Incendie Simplifiées

1 Vous êtes témoin d'un départ de feu

2 Déclenchez l'alarme depuis un déclencheur manuel

3 Alertez les pompiers (0)18 sur le poste interne ou 112 sur votre portable

4 Guidez et contrôlez l'évacuation en fermant les portes derrière vous



5 Mettez-en œuvre les moyens de secours pour limiter le développement et la propagation du feu

Ne jamais pénétrer dans un local sans aucune visibilité

Évacuation

1 Lors d'un départ de feu, appuyez sur le bouton d'alarme le plus proche. Sans témoin, les détecteurs de fumée déclenchent automatiquement l'alarme.

2 Dès que le signal d'alarme retentit, évacuez dans le calme, en suivant les guides d'évacuation et leurs instructions.

Le guide d'évacuation est chargé de rassembler et de faire sortir toutes les personnes qui suivent sa formation. Il les conduit au point de rassemblement.

3 Un serre-file s'assure que personne ne reste en arrière ou ne fait demi-tour.

Le responsable d'évacuation s'assure que le travail des guides et serre-files a été correctement réalisé, il est en lien avec les pompiers et met fin à l'alerte.

En l'absence du guide d'évacuation :

1 Dirigez-vous vers les sorties de secours en suivant le trajet indiqué sur les plans d'évacuation affichés à chaque étage et en vous aidant de l'éclairage de sécurité.

2 Rejoignez le point de rassemblement désigné pour votre site :

- **Site de la Fonderie**
  ↳ Cour supérieure
- **Site du Parlement**
  ↳ Place du Salin
- **Site des Fleurs**
  ↳ Rue des fleurs

Attention: Rejoignez le point de rassemblement désigné du lieu dans lequel vous vous trouvez.

Pour rejoindre le point de rassemblement :

- N'utilisez pas les ascenseurs.
- Ne revenez jamais en arrière.
- Si les fumées sont importantes, ne tentez pas de les affronter, baissez-vous (au sol, la visibilité et l'air sont meilleurs).
- Attendre l'autorisation du responsable sécurité pour réintégrer les locaux.

Important : Restez au point de rassemblement durant toute l'alerte jusqu'à la fin de l'alerte annoncée par le responsable d'évacuation.

Point de rassemblement

Issue de secours

Consignes en cas de Malaise ou d'Accident

Avant toute intervention et afin d'éviter un « sur accident » il faut écarter toute source de danger. Pour cela il convient de se protéger, protéger la victime ainsi que les personnes aux alentours.

Ensuite, en priorité, contactez :

Les secours internes

- Les Sauveteurs Secouristes du Travail (SST)
- Si vous ne trouvez pas de Sauveteur Secouriste du Travail, contactez l'accueil (05.61.36.81.00)

OU

Les secours externes

- Pompiers (18)
- SAMU (15)
- Zone sans réseau et n° d'appel européen (112)
- Pour les malentendants (114)

La personne référente de la Direction en cas de malaise ou accident à contacter: Chrystel Bodoira (06.30.50.40.94)

Le Message d'Alerte

Réalisez l'alerte à l'aide d'un téléphone portable ou à défaut d'un téléphone fixe. Précisez dans le message d'alerte :

- Votre identité et numéro d'appel
- Le lieu précis de l'accident : adresse, atelier, étage...
- La nature de l'accident : chute dans un escalier, malaise en cours...
- Le nombre de victimes
- L'état de la ou des victimes
- Les actions déjà engagées

Pour une bonne transmission du message :

- Répondre aux questions posées par les services de secours
- Ne jamais raccrocher le premier
- Si l'appel est réalisé par un tiers lui demander de revenir afin de rendre compte au SST
- Si possible, envoyer une personne à la rencontre des secours

Dans tous les cas, suivre les consignes données par les secours et organiser leur accès sur le lieu de l'accident, le plus près possible de la victime.

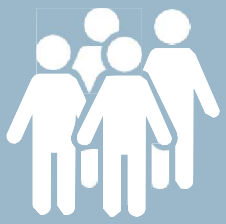
Consignes Vigipirate

1 S'échapper

Localisez le danger pour vous en éloigner

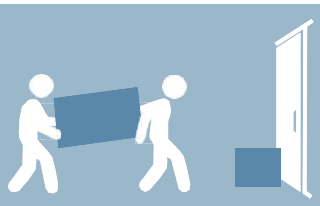
Si possible, aidez les autres personnes à s'échapper

Ne vous exposez pas



Alertez les personnes autour de vous et dissuadez-les de pénétrer dans la zone de danger

2 Se cacher



Enfermez-vous et barricadez-vous

Éteignez la lumière et coupez le son des appareils

Éloignez-vous des ouvertures et allongez-vous au sol

Sinon, abritez-vous derrière un obstacle solide (mur, pilier...)

Dans tous les cas coupez la sonnerie et le vibreur de votre téléphone

3 Alerter

Dès que vous êtes en sécurité, appelez le 17 ou le 112

Ne courez pas vers les forces de l'ordre et ne faites aucun mouvement brusque

Gardez les mains levées et ouvertes

Témoin d'une situation ou d'un **comportement suspect**, vous devez contacter les forces de l'ordre (17 ou 112). Quand vous rentrez dans un lieu, repérez les **sorties de secours**. Ne diffusez aucune information sur l'intervention des forces de l'ordre. Ne diffusez pas de rumeurs ou d'**informations non vérifiées** sur Internet et les réseaux sociaux. Sur les réseaux sociaux, suivez les comptes **@PlaceBeauvau** et **@gouvernementfr**.

Annexe 2 : Charte d'utilisation des systèmes d'information de l'ICT

La présente charte est un document juridique qui définit les règles d'usages et de sécurité que l'Institut Catholique de Toulouse (ICT) et l'utilisateur s'engagent à respecter dans l'utilisation des services et ressources informatiques internes : elle précise les droits et devoirs de chacun. Elle a également pour objet de sensibiliser les usagers aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées.

Préambule

Les systèmes d'information et du numérique (SIN) recouvrent l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'Institut Catholique de Toulouse (ICT) :
- Messagerie électronique ;
- Logiciels ;
- Serveurs ;
- ERP ;
- Internet ;
- Réseaux sociaux ;
- Plateformes collaboratives de travail et de services : Microsoft Teams, Moodle, etc.

L'informatique nomade tels les ordinateurs portables, les téléphones portables attribués au personnel habilité par l'établissement et fournis par l'ICT sont également des éléments constitutifs des SIN.

Le terme « utilisateur », désigne toute personne ayant accès, dans le cadre de l'exercice de son activité professionnelle ou pédagogique aux ressources du SIN quel que soit son statut.
Il s'agit notamment de :

- Tout personnel ou prestataire extérieur concourant à l'exécution de ses missions administratives et/ou pédagogiques ;
- Tout apprenant inscrit à l'ICT ou locataire d'un logement dans une des résidences du campus de l'ICT ;
- Tout alumni de l'ICT pour la messagerie électronique uniquement ;
- Tout personnel invité par l'ICT dans le cadre de coopération de recherche, d'enseignement ou de collaboration administrative.

I. Champs d'application

Les règles de bonnes pratiques informatiques et de sécurité, figurant dans la présente charte informatique, s'appliquent, à toute personne souhaitant se connecter au réseau informatique de l'ICT sur site ou à distance.

Le bon fonctionnement du Service des Systèmes d'Information et du Numérique (SSIN) suppose le respect par les utilisateurs de l'ensemble des dispositions législatives et réglementaires en vigueur (cf. liste ci-dessous, sans que cette liste soit limitative) :

I.1/ Les règlementations applicables

- La réglementation en matière d'ordre public, de bonnes mœurs, de droits des personnes : sont interdits notamment : les contenus à caractère violent, diffamatoire, injurieux, raciste, pornographique ou illicite qui seraient susceptibles de porter atteinte à l'intégrité ou à la sensibilité d'une autre personne ;
- La règlementation relative au respect de la vie privée des personnes (article R226-1 du code pénal et article 9 du code civil) : sont interdits notamment les contenus portant atteinte au droit à l'image, au droit au respect de la vie privée, les contenus à caractère diffamatoire, injurieux ;
- Le 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Toute violation expose son auteur à des sanctions disciplinaires et pénales conformément à la règlementation en vigueur, notamment au regard des articles 226-13 et 226-16 à 226-24 du code pénal ;

- La règlementation en matière de droits d'auteur (code de la propriété intellectuelle) ;
- En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat ;
- La règlementation en matière de fraude informatique (articles 323-1 et suivants du code pénal.)

I.2/ Les engagements de l'ICT

L'ICT porte à la connaissance de l'utilisateur la présente charte à son arrivée au sein de l'ICT.
De plus, elle est annexée au règlement intérieur des personnels et au règlement intérieur des apprenants, ce qui lui donne un caractère contraignant. L'utilisateur s'engage à en respecter les dispositions.
L'ICT facilite l'accès des utilisateurs aux ressources du SIN et met en œuvre toutes les mesures nécessaires pour assurer la sécurité du SIN et la protection des utilisateurs :

- Limite l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- Communique régulièrement aux utilisateurs les règles de bonnes pratiques informatiques par e-mails et actualise la présente charte informatique ;
- Respecte le droit à la déconnexion des salariés.

I.3/ Les engagements de l'utilisateur

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait des SIN de l'ICT auquel il a accès. Il accepte pleinement et sans aucune réserve la présente charte et s'engage pendant toute la durée d'utilisation des SIN à la respecter.

II. Règles d'utilisation des SIN

II.1/ Les conditions d'accès de l'utilisateur

Le contrôle d'accès logique permet d'identifier toute personne utilisant un ordinateur.
Sont données :
- une identification administrative (login + mot de passe) à chaque salarié ayant une charge administrative ;
- et/ou une identification pédagogique à chaque utilisateur ayant une activité pédagogique et à tout apprenant inscrit à l'ICT.

L'identification constitue une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Ainsi à chaque connexion, l'utilisateur se voit attribuer des droits propres sur les ressources du SIN dont il a besoin pour son activité. Ce droit d'accès est donc strictement personnel et incessible.
Il cesse lorsque l'utilisateur quitte l'ICT ou s'il est constaté qu'il a violé l'une des obligations de la présente charte.
Le droit d'accès n'est conféré à l'utilisateur qu'aux fins d'une utilisation compatible avec les activités de l'ICT, qu'elles soient administratives, pédagogiques ou de recherche. Elle exclut tout autre utilisation, notamment commerciale.
L'utilisateur reconnait que l'usage de son droit d'accès peut engager sa responsabilité dans les conditions précisées dans la présente charte.
Toute violation des conditions d'accès décrites dans la charte, outre les sanctions disciplinaires, peut engager la responsabilité civile de son auteur et constituer une infraction au sens des articles 323-1 à 323-7 du code pénal.

II.2/ La politique de protection des données personnelles

II.2.1/ La protection des utilisateurs des SIN

- L’utilisation du SIN peut nécessiter la communication de données à caractère personnel. On entend par données à

  caractère personnel toute donnée permettant d’identifier un individu directement ou indirectement, sous quelque forme que ce soit.

L’ICT se conforme à la loi n°78-17 du 6 janvier 1978 modifiée dite « loi informatique et libertés » et au règlement européen N° 76-679 du 27 avril 2016 dit RGPD.
Les données personnelles collectées et traitées ont pour but de :

- Constituer un annuaire des comptes utilisateurs pour rendre possible un accès aux ressources informatiques mises à disposition sur les réseaux filaires et hertziens de l’ICT ;
- Permettre un accès authentifié aux ressources et services informatiques mis en œuvre sur le réseau informatique de l’ICT ;
- Respecter la réglementation, en particulier pour la détection et la lutte contre les infractions pénales lors de la circulation des données sur Internet, notamment la messagerie ou la navigation Web ;
- Assurer le stockage et/ ou l’archivage des fichiers/ courriers électroniques/ données de recherche sensibles que l’utilisateur souhaite conserver uniquement sur des supports professionnels agréés par le SSIN de l’ICT.

Conformément à ces dispositions, chaque utilisateur des SIN dispose d’un droit d’accès, de rectification, de limitation et d’effacement dans la mesure possible, relatif à l’ensemble des données le concernant, y compris les données portant sur l’utilisation des SIN.
Ces droits s’exercent auprès du délégué à la protection des données à l’adresse dpo@ict-toulouse.fr, et un recours auprès de la CNIL est possible pour l’utilisateur s’il considère que ses droits ne sont pas respectés.

II.2.2/ Le respect de la réglementation relative à la protection des données par les utilisateurs des SIN

L'utilisateur des SIN est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n 78-17 du 6 janvier 1978 dite « Informatique et Libertés » modifiée par la loi n 2004-801 du 6 aout 2004 et aux directives du RGPD.

- 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 » et le Règlement (RGPD) ;
- En conséquence, tout utilisateur des SIN souhaitant procéder à une telle création devra en informer préalablement les services compétents, notamment le délégué à la gestion des données personnelles (DPO), à l’adresse mail suivante : dpo@ict-toulouse.fr. Le DPO prendra les mesures nécessaires au respect des dispositions légales.

L’'ICT, conformément à son obligation légale issue de l’article 5 du RGPD, a mis en place un système de journalisation des accès Internet, de la messagerie et des données échangées afin de détecter sur les systèmes informatiques les incidents, les intrusions et les utilisations non autorisées ou détournements effectués par les usagers.
L'ICT se réserve le droit de mettre en place si besoin des outils de traçabilité sur tous les systèmes d'information. Préalablement à cette mise en place, l'ICT en avertira les instances représentatives du personnel et procédera, à une déclaration sur son registre de traitement

CNIL, qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n 78-17 du 6 janvier 1978 modifiée par la loi n 2004-801 du 8 aout 2004.

II.3/ Les règles de bonnes pratiques de sécurité du poste de travail à l'ICT

Quel que soit l'appareil, l'utilisateur doit faire preuve de prudence et suivre les bonnes pratiques d'utilisation du poste de travail. Aussi il ne doit pas :

- Accéder ou tenter d'accéder à des ressources du SIN, pour lesquelles il n'a pas reçu d'habilitation explicite : les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est confiée ;
- Connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'ICT. Toute connexion aux réseaux locaux de l'ICT de matériels personnels présente un risque, leur niveau de sécurité n'étant ni maîtrisé ni vérifiable ;
- Être vigilant aux diverses tentatives d'hameçonnage ;
- Ne pas utiliser son login professionnel ICT à des fins personnelles ;
- Installer, télécharger ou utiliser sur le matériel de l'ICT, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation du SIN ;
- Apporter directement ou indirectement des perturbations au fonctionnement du réseau et du SIN auxquels il accède et provoquer des modifications, altérations ou destructions concernant des données ou des fichiers autres que ceux dont il est l'auteur ;
- Reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits ;
- Copier des œuvres protégées par le droit d'auteur.

L'utilisateur s'engage à :

- Respecter les règles de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie ;
- N'installer que les applications nécessaires et toujours avec l'autorisation du SSIN ;
- Faire des sauvegardes régulières sur le réseau de l'ICT ;
- Se conformer aux dispositifs mis en place par l'ICT pour lutter contre les virus et les attaques par programmes informatiques ;
- Signaler tout acte ou toute suspicion d'acte de malveillance constaté sur les appareils utilisés, qu'ils soient professionnels ou personnels s'il y a eu connexion sur le réseau ou sur un service en ligne de l'ICT.

II.4/ La politique de l'ICT d'authentification et de gestion des accès aux comptes utilisateurs

II.4.1/ La politique générale

L'identification unique constitue une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Ainsi, à chaque connexion, l'utilisateur se voit attribuer des droits propres sur les ressources du SIN dont il a besoin en fonction de son activité (administrative et/ou pédagogique).

- Chaque mot de passe doit être modifié selon la fréquence suivante : tous les 6 mois ;
- Un mot de passe pour être efficace doit comporter au moins 12 caractères alphanumériques de 4 types différents, dont au moins des majuscules, des

minuscules, des chiffres et des caractères spéciaux.

- Il ne doit pas :
  - Être identique au login, même en inversant les caractères ;
  - Comporter des informations sur l'utilisateur (nom, prénom numéro de téléphone, date de naissance de l'utilisateur, etc.) ;
  - Être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu ;
  - Être enregistré sur un simple fichier mais dans l'application « KEEPASS » installée sur les ordinateurs de l'ICT ;
  - Être communiqué à un tiers : les login et mot de passe sont strictement confidentiels. L'utilisateur est personnellement responsable de l'utilisation qui peut en être faite, et ne doit à aucun moment la communiquer.
- L'utilisateur doit respecter la gestion des accès, en particulier ne pas utiliser les login et mot de passe d'un autre utilisateur, ni chercher à les connaître.

Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de donner son mot de passe, il devra procéder, dès que possible, au changement de ce dernier ou en demander la modification à l'administrateur.

- L'utilisateur doit privilégier des mots de passe uniques pour chaque service, site et logiciel utilisé. Il est recommandé de ne pas se servir d'un mot de passe déjà utilisé pour un outil personnel. Utiliser le même mot de passe pour tous les sites ne fait qu'augmenter le risque informatique.

II.4.2/ La politique relative au télétravail

Pour des raisons de sécurité, le travail à distance pour les salariés éligibles au télétravail, n'est possible que suivant les modalités suivantes :

- Connexion uniquement à partir d'un ordinateur mis à disposition par l'ICT, protégé par un réseau privé virtuel (VPN), pour la réalisation de son activité professionnelle ;
- Double authentification pour la connexion via l'application Fortitoken, à installer sur le téléphone personnel de l'utilisateur en télétravail, afin de recevoir le code d'authentification ;
- Application des mises à jour de sécurité sur l'ensemble des équipements professionnels et ce dès qu'elles sont proposées (PC).

L'utilisation d'outils personnels pour la réalisation d'une activité professionnelle est déconseillée.

II.5/ Les règles d'utilisation de la messagerie électronique

L'utilisation de la messagerie constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'ICT.
L'ICT met à disposition de l'utilisateur une boîte à lettres professionnelle nominative ou partagée, lui permettant d'émettre et de recevoir des messages électroniques et ne peuvent être utilisées qu'à des fins professionnelles.
La gestion d'adresses électroniques correspondant à des listes de diffusion institutionnelles, désignant une catégorie ou un groupe d'utilisateurs, relève de la responsabilité exclusive de l'ICT : ces adresses ne peuvent être utilisées sans autorisation explicite.

Les e-mails et les pièces jointes ont un rôle prépondérant dans la fraude informatique. L'utilisateur doit être particulièrement vigilant quand il utilise sa messagerie professionnelle et se méfier des tentatives d'hameçonnage ou phishing. Ces techniques consistent pour un hacker à envoyer un e-mail frauduleux pour inciter le destinataire du message à divulguer

des informations personnelles, en se faisant passer par exemple pour un organisme ou un tiers connu.
L'utilisateur doit :

- Vérifier l'expéditeur de l'e-mail et en cas de doute alerter le service informatique de l'ICT support@ict-toulouse.fr
- S'interdire d'ouvrir des e-mails ou des pièces jointes provenant d'expéditeurs inconnus ou suspects ;
- Protéger son identité numérique pour limiter les risques de fraude.

Par ailleurs, conformément au code pénal, l'utilisateur ne doit pas diffuser d'informations ou données dont le contenu présente un caractère illégal, notamment raciste, diffamatoire ou injurieux. La consultation de sites à contenu pornographique depuis les locaux de l'ICT est interdite.

II.5.1/ La sécurisation du partage des données

Un message envoyé via Internet (mail, Teams, ...) peut potentiellement être intercepté, même illégalement et lu par n'importe qui.

Il est interdit d'utiliser des sites de partage de données volumineuses non sécurisées de type We Transfer, Dropbox ou autres.
Seule l'utilisation de FILESENDER géré par le GIP RENATER, service de transfert de fichiers de la communauté Enseignement Supérieur et Recherche, est autorisée pour l'envoi de fichiers volumineux ou contenant des données sensibles ou confidentielles, car elle permet un chiffrement des données. Elle offre un espace de stockage temporaire à destination des personnels de l'ICT et à leurs interlocuteurs privilégiés. Elle garantit :

- Une authentification via la fédération d'identité Education-Recherche sur laquelle l'ICT est référencée ;
- Un dépôt temporaire de fichiers (jusqu'à 100 fichiers pour une taille maximale de dépôt de 100 Go; taille maximale de fichier pour les navigateurs non compatibles HTML.5 : 2 Go ;
- expiration des dépôts : maximum 30 jours), à destination d'un ou plusieurs correspondants (jusqu'à 50 adresses e-mails séparées par une virgule ou un point-virgule) ;
- Un chiffrement de bout en bout certifié par l'ANSSI ;
- Une consultation des fichiers déposés et leur téléchargement ;
- Une invitation de correspondants qu'ils soient en France ou à l'étranger, à déposer des fichiers dans son espace personnel de dépôt de fichiers (expiration des invitations : maximum 30 jours).

II.5.2/ L'utilisation privée de la messagerie électronique

L'utilisation résiduelle de la messagerie électronique à titre privé est tolérée si elle est non lucrative et raisonnable, tant dans sa fréquence, son volume que dans sa durée.
Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.
Tous les messages présents dans la boîte mails sont réputés professionnels à l'exclusion de ceux explicitement désignés par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de mentionner le caractère privé d'un message en objet et de le stocker dans un répertoire identifié comme ayant un caractère privé, en utilisant les mots clés PRIVE ou PERSONNEL.
La sauvegarde régulière des messages à caractère privé incombe à l'utilisateur.

II.5.3/ La consultation du compte de messagerie électronique par l'ICT

« Les fichiers créés, envoyés ou reçus depuis le poste de travail mis à disposition par l'employeur ont par principe un caractère professionnel ».

Ainsi, l'ICT peut consulter y compris en dehors de la présence du salarié, tout courrier électronique reçu ou envoyé par ce dernier depuis sa messagerie professionnelle. En revanche, l'ICT a l'interdiction de consulter et ce même en présence du salarié, les messages portant la mention « Personnel » ou « Privé » ou stockés dans un répertoire portant ces mentions.
Cette protection connaît toutefois une exception : si l'ICT peut justifier de « circonstances particulières » lui permettant de solliciter une autorisation judiciaire d'accéder aux e-mails personnels ou privés du salarié ou si une enquête judiciaire est en cours.

Droit de consultation de l'ICT de la messagerie du salarié et continuité de service

Continuité de service et absence prolongée
En cas d'absence prolongée (vacances, maladie, mise à pied conservatoire...) : dans le cas où le salarié absent détient sur son poste des informations indispensables à la poursuite de l'activité du service, l'ICT peut exiger la communication des identifiant et mot de passe du salarié, si l'administrateur réseau n'est pas en mesure de lui fournir l'accès au poste de ce salarié *(CNIL/contrôle de l'utilisation d'internet et de la messagerie électronique*).
Dans ce cas les messages, sauf ceux identifiés comme personnels ou privés, seront récupérés par le responsable.
Un message automatique pourra être envoyé à partir de la boîte mail du salarié afin de donner les noms des personnes à contacter en l'absence du salarié, permettant ainsi d'assurer la continuité du service.

Continuité de service et départ du salarié
Dans le cas d'un départ définitif et programmé du salarié (démission, rupture conventionnelle, licenciement avec préavis, départ à la retraite…), l'accès du salarié, y compris l'accès à distance à son compte de messagerie est désactivé le lendemain du dernier jour de son préavis de départ, même si le préavis n'a pas été exécuté.

Le collaborateur doit vider son compte de messagerie professionnelle de tout mail/ répertoire identifié comme personnel ou privé, avant sa date de départ.

La date de fermeture du compte de messagerie du salarié est fixée au dernier jour du contrat du salarié + 6 mois pour des raisons de continuité de service.
Sur décision du responsable hiérarchique une information et une redirection des messages vers l'adresse du service ou une adresse nominative durant ces 6 mois est réalisée afin d'assurer la continuité du service.
Au terme de ce délai l'adresse nominative de messagerie électronique du salarié est supprimée.

Dans le cas d'un départ non programmé, le salarié est informé par son N+1, de la date de fermeture de sa messagerie dans un délai raisonnable, afin qu'il puisse s'organiser et qu'il puisse récupérer uniquement ses messages identifiés comme personnels ou privés, ce sous le contrôle d'un tiers de confiance.
La messagerie devra être définitivement fermée à la date indiquée par le N+1.

Mise à pied conservatoire et suspension de l'accès du salarié à sa messagerie professionnelle
En cas de mise à pied conservatoire (mesure préventive, immédiate et provisoire prise par l'employeur en cas de manquement grave commis par le salarié rendant impossible sa présence à l'ICT, le temps de décider du sort du collaborateur), l'accès du salarié à sa messagerie professionnelle sera suspendu par l'ICT le temps de la mise à pied conservatoire du salarié.

Conservation des e-mails

Type d'e-mail	Durée de conservation	Base légale ou réglementaire
E-mails relatifs à la gestion du personnel	Jusqu'à 5 ans après la fin du contrat	Code du travail
E-mails commerciaux	3 ans minimum	Obligations comptables et fiscales
E-mails fiscaux	6 à 10 ans	Obligations comptables et fiscales
E-mails contenant des données personnelles	Durée nécessaire selon finalité	RGPD
E-mails relatifs aux contrats de travail	Toute la durée du contrat + 5 ans	Code du travail
E-mails concernant les litiges	Jusqu'à résolution + 5 ans	Précautions légales
Correspondances liées à des projets spécifiques	Durée du projet + 3 ans	Gestion de projet
E-mails de formation et de développement professionnel	2 ans après la dernière utilisation	Gestion des ressources humaines
E-mails liés à la santé et sécurité au travail	Toute la durée de l'emploi + 5 ans	Code du travail, RGPD
E-mails relatifs aux réclamations clients	5 ans après la résolution	Gestion clientèle, RGPD
Correspondance interne importante	Indéfiniment ou selon politique interne	Gestion d'entreprise
E-mails liés aux enquêtes internes	Au moins 5 ans après fin de l'enquête	RGPD, droit du travail
E-mails concernant les droits d'auteur et propriété intellectuelle	Jusqu'à 70 ans après mort de l'auteur	Droit d'auteur, propriété intellectuelle
E-mails relatifs aux contrôles et audits	10 ans	Réglementations financières et comptables
E-mails contenant des informations financières annuelles	Au moins 10 ans	Obligations comptables et fiscales
E-mails liés aux assurances et polices d'assurance	Durée de la police + 10 ans	Droit des assurances

II.6. Les règles d'utilisation d'Internet

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur dont la liste est rappelée au paragraphe I.1 p.3.

L'utilisation d'Internet constitue un élément essentiel d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'ICT.
L'ICT met à la disposition de l'utilisateur un accès Internet chaque fois que cela est possible. Internet est un outil de travail ouvert à des usages professionnels (administratifs et pédagogiques).

Sécurité :

- L'utilisateur doit vérifier la sécurité des sites consultés et privilégier les sites officiels et les sites dont l'adresse commence par « https://
- L'ICT se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

II.7. Les règles d'utilisation des réseaux sociaux

Il est rappelé que l'utilisation des réseaux sociaux est soumise à l'ensemble des règles de droit en vigueur dont la liste est rappelée au paragraphe I.1 p.3.

Le fait de révéler par le biais des réseaux sociaux des informations confidentielles, de publier des images de l'entreprise ou de ses membres sans autorisation préalable, ou de tenir des propos concernant l'ICT ou ses membres dépassant le cadre de la liberté d'expression est susceptible d'entraîner des sanctions disciplinaires voir pénales.

Tout propos tenu sur un réseau social engage la responsabilité de son auteur, et ne constitue en rien une déclaration officielle de l'ICT.

Par ailleurs, si un utilisateur est contacté via un réseau social, il doit s'assurer de l'identité du demandeur d'informations : à l'instar du phishing (hameçonnage), des demandes d'informations personnelles peuvent se faire via les réseaux sociaux, par des interlocuteurs qui peuvent évoquer des situations d'urgence, des demandes de confirmation, etc.

III. Règles de sécurité du SIN

III.1 Devoirs de signalement et d'information

L'utilisateur doit avertir le SSIN dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte dans le système d'information.

III.2 Mesures de contrôle et de sécurité

Le SSIN assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de l'ICT. Les membres de ce service disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place dans le respect de la législation applicable.
Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que :

- ces informations sont couvertes par le secret des correspondances ou qu'identifiées comme telles, elles relèvent de la vie privée de l'utilisateur ;
- elles ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, elles ne tombent pas dans le champ de l'article 40 alinéa 2 du code de procédure pénale.

III.2.1 Procédure en cas de cyber-malveillance

L'hameçonnage ou *phishing* est un SMS ou mail frauduleux destinés à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires (comptes d'accès, mots de passe…) en se faisant passer pour un tiers de confiance.

1. **<u>Les règles de bonnes pratiques informatiques contre une tentative de *phishing*</u> :**

- **1. Ne jamais communiquer d'informations sensibles par messagerie ou téléphone :** Aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

- **2. Avant de cliquer sur un lien douteux,** positionner le curseur de la souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou aller directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

- **3. Vérifier l'adresse du site qui s'affiche dans son navigateur.** Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour tromper l'utilisateur. Au moindre doute, ne fournir aucune information et fermer immédiatement la page correspondante.

- **4. En cas de doute, contacter le SSIN immédiatement.**

- **5. Utiliser des mots de passe différents et complexes** pour chaque site et application, afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes.

- **6. Si le site le permet, vérifier les date et heure de dernière connexion à votre compte** afin de repérer si des accès illégitimes ont été réalisés.

- **7. Si le site vous le permet, activer la double authentification pour sécuriser vos accès.**

III.2.3 Procédure en cas de cyberattaque

Pour vous informer sur les bonnes pratiques
et les principales menaces en matière de cybersécurité
rendez-vous sur :
www.cybermalveillance.gouv.fr

IV. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et sans préjuger des poursuites ou sanctions pénales, il pourra être décidé de mesures visant à limiter les usages, à titre conservatoire, et de sanctions disciplinaires.

V. Entrée en vigueur de la charte

La présente charte est annexée au règlement intérieur de l'ICT qui a été validé au Conseil d'Établissement de l'ICT le 15/05/2024.

Toulouse, le 19 juin 2024

Professeur François Moog
Recteur de l'Institut Catholique de Toulouse

Annexe 3 : Politique d'inclusion et d'accessibilité

ÉTUDIER A L'ICT EN SITUATION DE HANDICAP : NOTRE POLITIQUE D'INCLUSION

L'objectif est de développer une démarche qualité inclusive afin de garantir à tous les apprenants issus de la formation initiale ou de la formation professionnelle portant un handicap, l'accessibilité dans toutes ses dimensions au sein de l'ICT (accessibilité aux locaux, accès à l'information, au savoir, à la vie étudiante, aux études, au pôle Compétences, à la Bibliothèque, aux Relations internationales, au Pôle culturel, etc.). L'apprenant en situation de handicap doit bénéficier de l'ensemble des services de droit commun que met à disposition l'ICT.

La question de l'inclusion est inscrite dans la politique RSE de l'établissement et la dimension handicap – visible ou moins visible – revêt une importance toute particulière. Il s'agit d'abord de mettre en place et améliorer les dispositifs d'accueil, d'accompagnement et de feedback des étudiants en situation de handicap. Cela se renforce d'un développement des partenariats avec des entités extérieures (prestataires, entreprises, associations, collectivités territoriales) permettant le maillage d'un réseau mobilisable.

La Mission handicap de l'ICT est organisée en conformité avec le cadre législatif : loi du 11 février 2005, circulaire n° 2011-220 du 27 décembre 2011 : Examens et concours de l'enseignement scolaire et de l'enseignement supérieur et la Charte université handicap du 19 avril 2012.

ACCUEILLIR ET ACCOMPAGNER : LE RÔLE DE LA MISSION ACCUEIL HANDICAP

Interface entre l'apprenant en situation de handicap et les différents acteurs de l'établissement (équipes administratives et pédagogiques), le rôle de la Mission Accueil Handicap est de superviser et veiller au respect des aménagements préconisés par le Service Interuniversitaire de Médecine Préventive et de Promotion de la Santé (SIMMPS) afin que l'apprenant puisse suivre son cursus d'étude dans les meilleures conditions possibles.

UNE MISSION D'ACCUEIL

En début d'année universitaire, une étude des besoins spécifiques des apprenants (étudiants en formation continue et professionnelle) en situation de handicap est réalisée, après visite préalable à la Médecine Préventive. Nous mettons alors en place un suivi adapté et des aménagements, en lien avec les différents acteurs et partenaires : équipes pédagogiques et administratives, Service Interuniversitaire de Médecine Préventive et de Promotion de la Santé (SIMPPS), Pôle Compétences et partenaires extérieurs.

Une fiche de liaison reflétant la notification du SIMPSS sera alors délivrée pour validation du protocole MAH de l'apprenant de l'ICT. Il est indispensable de prendre ces contacts au plus tôt afin de pouvoir bénéficier des aménagements dès la rentrée.

Les mesures d'accompagnement sont ajustées en fonction de l'évolution de l'état de santé de l'apprenant et/ou de l'apparition de nouveaux besoins liés à la formation.

QUELQUES EXEMPLES D'AMENAGEMENTS POSSIBLES (liste non-exhaustive)

- Temps d'épreuve majoré ;
- Soutien pédagogique (tutorat) ;
- Preneur de notes (apprenant aidant) ;
- Mise à disposition de matériel (ordinateur, logiciels, etc.) ;
- Adaptations de documents (agrandissement, etc.) ;
- Aménagement de cursus ;
- Supports adaptés ;
- Temps de pause ;
- Salle à part ou à petit effectif ;
- Secrétariat d'examens ;
- Photocopies gratuites.

UNE MISSION D'ACCOMPAGNEMENT

Nous proposons un certain nombre de dispositifs ainsi qu'un maillage auprès des équipes administratives et pédagogiques par le réseau des correspondants-relais handicap (CRH), interlocuteurs privilégiés au sein des facultés et organismes. Nous travaillons également avec des partenaires extérieurs dans un réseau mobilisable.

Afin d'optimiser l'opérationnalisation des aménagements et de leur suivi, nous insistons tout au long de l'année sur des actions de sensibilisation à destination de l'ensemble de la communauté ICT (apprenants et équipes) ainsi que des formations spécifiques auprès des personnels (administratifs, pédagogiques). Le suivi qualité est assuré par des questionnaires de satisfaction permettant d'apporter les remédiations éventuelles.

DISPOSITIFS EXISTANTS (liste non-exhaustive)

- Éducatrice spécialisée à destination des apprenants en situation d'autisme ;
- Cellule d'écoute psychologique ;
- Ateliers de gestion du stress, de la concentration, etc.
- Actions de sensibilisation thématiques.

Accompagner les apprenants en situation de handicap est une mission essentielle de notre établissement. L'ICT souhaite garantir à ces derniers l'accès à tous les aspects de la vie universitaire et rappeler que cet accueil est l'affaire de tous.

ACCEDER ET PARCOURIR : UNE UNIVERSITE ACCESSIBLE

Dans ce lieu chargé d'histoire, la politique d'accessibilité et d'inclusion de l'Institut Catholique de Toulouse vise à prendre en considération l'accessibilité comme un élément fondamental d'un campus adapté à ses apprenants.

ACCESSIBILITE DES LOCAUX

Dans le respect des normes en vigueur, les locaux de l'ICT sont accessibles aux personnes à mobilité réduite. Les ascenseurs, les chaises d'évacuation, les flashs lumineux (dans les sanitaires notamment) sont régulièrement inspectés.

Des registres d'accessibilité sont disponibles et consultables à l'accueil des trois sites.

Important : connaissant actuellement une période de travaux, notre établissement a reçu l'approbation d'un agenda d'accessibilité programmée.

ACCESSIBILITE NUMERIQUE

De nombreux ordinateurs sont disponibles, notamment dans les espaces de coworking, sur les heures d'ouverture de l'établissement. Un parc d'ordinateurs portables est également mis à disposition des apprenants pour la rédaction de leurs épreuves de contrôle continu et/ou de partiels, ou pour une prise en main numérique.

Une réflexion a été engagée au sujet d'une demande d'agrément permettant de bénéficier de la plateforme PLATON pour la bibliothèque universitaire de l'ICT.

Annexe 4 : Propriété intellectuelle et fraude

L'utilisation des ressources documentaires (ressources numériques, papier, etc.) implique le respect des droits de propriété intellectuelle de l'auteur ainsi que ceux de ses partenaires et plus généralement, de tous les tiers titulaires de tels droits.
En conséquence, chaque utilisateur doit :

- Utiliser les logiciels dans les conditions des licences souscrites ;
- Ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, documents issus de pages internet, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

Un travail oral ou écrit rendu par un apprenant doit représenter ses propres efforts ou ceux de son groupe.
Il y a donc fraude si l'apprenant ou son groupe exploite le travail d'autrui ou produit un contenu par un outil d'intelligence artificielle générative (par exemple ChatGPT) comme s'il s'agissait de son propre travail. Il est particulièrement interdit de :

- Utiliser les termes exacts d'une publication sans la citer entre guillemets et d'identifier clairement la source (en note de bas de page, par exemple) ;
- Paraphraser ou reformuler un concept, une recherche ou interpréter des idées (verbales ou écrites) d'une autre personne morale ou physique, sans la citer et identifier la source, à titre gracieux ou payant ;
- Présenter des données de recherche qui ont été falsifiées ou inventées de quelque façon que ce soit ;
- Présenter sans autorisation écrite préalable des professeurs concernés, le même travail ou une partie importante d'un même travail dans plus d'un cours ou un autre travail déjà présenté ailleurs ;
- Falsifier une évaluation universitaire ou la dénaturer ;
- Utiliser une pièce justificative qui aurait été contrefaite ou falsifiée afin d'en dévier l'utilisation normale ;
- Recopier les données produites par un outil d'intelligence artificielle générative (par exemple ChatGPT…) sans citer l'outil utilisé ainsi que la transcription des contenus générés par l'IA.

Les travaux de groupe sont soumis aux mêmes règles d'intégrité intellectuelle que les travaux individuels. En cas de non-respect des règles déontologiques, le groupe est considéré comme solidaire devant la fraude. Il pourra être sanctionné.

L'ICT est doté d'un logiciel de détection des similitudes et des contenus générés par l'IA générative, Compilatio (https://www.compilatio.net/). Cet outil recherche et quantifie (taux en pourcentage de similitudes) dans le document analysé des similitudes avec des documents sources (pages internet, publications scientifiques, documents ajoutés par les enseignants de l'ICT) et des contenus produits par l'intelligence artificielle générative.

L'interprétation des résultats et l'étude des passages similaires est à l'appréciation de l'enseignant correcteur.

Annexe 5 : Associations étudiantes et vie étudiante

PRINCIPES GENERAUX

Les associations apprenantes exercent leurs activités dans des conditions qui ne portent pas atteinte aux activités d'enseignement et de recherche et qui ne troublent pas l'ordre public. Sont prohibées toutes activités qui constitueraient des actes ne respectant pas la charte de l'ICT. Les activités commerciales ne peuvent se dérouler qu'avec l'autorisation de la direction de l'ICT et dans le respect des statuts de l'association et de la règlementation, notamment fiscale et comptable, en vigueur. Les activités contraires au respect des lois sur l'informatique sont interdites. Les associations apprenantes sont responsables des locaux et du matériel mis à leur disposition. De manière générale, l'ICT se réserve le droit de suspendre toute manifestation, notamment en cas de troubles à l'ordre public, d'atteintes à l'hygiène et à la sécurité ou de mise en danger des personnes.

PRINCIPES DE RECONNAISSANCE DES ASSOCIATIONS ETUDIANTES PAR L'ICT

Peuvent demander une reconnaissance les associations dont les activités principales s'exercent à l'ICT, dont les projets ont un impact sur les apprenants de l'ICT et dont la majorité des membres du bureau a la qualité d'apprenant de l'ICT.

PROCEDURE DE RECONNAISSANCE DES ASSOCIATIONS ETUDIANTES PAR L'ICT

Les associations qui souhaitent obtenir la reconnaissance doivent être juridiquement des associations de type loi 1901 qui respectent les obligations légales et dont les statuts ont été déposés auprès de la préfecture. L'association dépose ensuite la copie de ces documents accompagnés de la copie du récépissé de dépôt délivré par la préfecture auprès du service de la Vie étudiante de l'ICT et du Rectorat de l'ICT. L'association doit également apporter la preuve qu'elle a bien souscrit une assurance responsabilité civile couvrant ses missions statutaires. Le BVE (avec l'aide du Secrétaire Général, du Vice-Recteur à la vie étudiante et au développement académique et du Directeur de la communication) vérifie si l'objet de l'association est conforme aux principes généraux de la reconnaissance.

Le Vice-Recteur à la vie étudiante et au développement académique est ensuite informé et soumet l'approbation de la reconnaissance au Recteur de l'ICT. Le CVU (Conseil de la Vie Universitaire) est informé une fois par an de la liste des associations apprenantes bénéficiant de la reconnaissance.

DUREE ET RENOUVELLEMENT DE LA RECONNAISSANCE

La reconnaissance est accordée pour une année universitaire. Les associations doivent renouveler leur demande chaque année avant le 15 novembre. Les changements de statuts et de composition du bureau de même que la dissolution de l'association doivent être signalés sans délais au BVE et au Vice-Recteur à la vie étudiante et au développement académique. Chaque année, au plus tard au moment de la demande de renouvellement, l'association doit présenter au Vice-Recteur à la vie étudiante et au développement académique un bilan écrit concernant les actions menées au cours de l'année écoulée ainsi qu'un bilan financier, et fournir une attestation d'assurance valable pendant toute l'année universitaire en cours.

DOMICILIATION DES ASSOCIATIONS A L'ICT

Les associations reconnues peuvent demander à être statutairement domiciliées à l'ICT. La demande est adressée au Vice-Recteur à la vie étudiante et au développement académique et validée par le Recteur de l'ICT. L'autorisation de domiciliation n'a pas pour effet l'attribution d'un local.

MISE A DISPOSITION DE LOCAUX

Des locaux de l'ICT, peuvent aussi être mis à disposition de façon plus régulière pour accueillir les activités courantes et journalières des associations. Ces locaux sont attribués prioritairement aux associations contribuant de façon régulière à l'animation de la communauté universitaire. Des locaux peuvent être mis à

disposition des associations apprenantes à titre ponctuel pour le déroulement d'un projet particulier (conférences, rencontres diverses, stands d'information, manifestations culturelles ou sportives, etc.).

MISE A DISPOSITION TEMPORAIRE DE LOCAUX

Les associations peuvent demander à réserver des locaux de l'ICT pour le déroulement de leurs activités spécifiques pendant les horaires d'ouverture de l'établissement. Une demande de réservation présentant l'objet de l'activité doit être adressée au bureau de la Vie étudiante (BVE). Aucune manifestation apprenante ne peut se dérouler sans que l'accord écrit lui ait été signifié. Le délai minimum pour déposer une demande est de 15 jours avant la date de la manifestation projetée.

ENGAGEMENT ETUDIANT

Conformément au décret n° 2017-962 du 10 mai 2017 relatif à la reconnaissance de l'engagement des étudiants dans la vie associative, sociale ou professionnelle, les apprenants ont la possibilité de valoriser des activités associatives, sociales ou professionnelles mentionnées à l'article L. 611-9 du code de l'éducation : « activité bénévole au sein d'une association régie par la loi du 1er juillet 1901 relative au contrat d'association ou inscrite au registre des associations en application du code civil local applicable dans les départements du Bas-Rhin, du Haut-Rhin et de la Moselle, activité professionnelle, une activité militaire dans la réserve opérationnelle prévue au titre II du livre II de la quatrième partie du code de la défense, engagement de sapeur-pompier volontaire prévu à l'article L. 723-3 du code de la sécurité intérieure, service civique prévu au II de l'article L. 120-1 du code du service national ou volontariat dans les armées prévu à l'article L. 121-1 du même code ».

À cela s'ajoutent les activités suivantes : engagement solidaire et bénévolat, activités d'engagement étudiant (associations estudiantines), implication dans les projets culturels de l'ICT, projets d'initiative professionnelle, etc. Un dispositif de valorisation sous forme de bonification est mis en place, garantissant la validation, pour l'obtention d'un diplôme, des compétences, connaissances et aptitudes acquises par leurs apprenants. Pour bénéficier d'une bonification, l'apprenant présente la demande de validation de l'Engagement Étudiant pour accord par une commission avant la date définie chaque année. A la fin de l'année universitaire (selon la date définie chaque année), l'apprenant doit présenter son Dossier Personnel d'Engagement Étudiant (DPEE) dûment complété. La validation de l'Engagement Étudiant s'accompagne d'une inscription dans l'annexe descriptive au diplôme.

VENTES EXCEPTIONNELLES ET OPERATIONS PROMOTIONNELLES DIVERSES

Les associations respectent le principe de neutralité commerciale de l'ICT. Ainsi, la vente de produits dans I 'enceinte de I 'université à l'initiative des apprenants doit revêtir un caractère exceptionnel et être directement liée à une activité étudiante. Ils peuvent être ponctuellement autorisés à organiser dans ou devant les bâtiments d'enseignement, des évènements impliquant des échanges commerciaux de faible envergure (opérations petits déjeuners, ventes de gâteaux, tombolas...). Toutefois ces dernières sont limitées à 5 manifestations par an et par association. L'association en fait la demande auprès du BVE au moins 15 jours avant la (les) date(s) projetées. La décision est matérialisée par un courrier d'autorisation mentionnant les conditions d'exercice de ces activités.

ESPACES D'AFFICHAGE ET DISTRIBUTION DE TRACTS : LA DIFFUSION D'INFORMATIONS EST EGALEMENT POSSIBLE SUR LE SITE DE L'ICT

L'association est responsable des affichages et des distributions de documents réalisés par ses membres. Les affiches et documents doivent être directement liés à l'objet de l'association et porter son sigle ou logo. Le droit d'affichage est strictement limité aux panneaux prévus à cet usage ou en libre accès. Toute utilisation du logo de l'ICT, sur un support papier ou électronique, devra faire l'objet d'une autorisation préalable accordée par le Vice-Recteur à la vie étudiante et au développement

académique et la Direction de la communication sur demande auprès du BVE formulée au moins 15 jours avant la date d'impression/diffusion projetée. Tout affichage ne respectant pas les valeurs et règles de l'ICT sera automatiquement retiré par l'administration.

UTILISATION DES RESSOURCES NUMERIQUES DU CAMPUS (RESEAU/MESSAGERIE)

En matière d'utilisation des ressources du réseau en général et de la messagerie en particulier, les associations sont soumises au respect des dispositions de la charte informatique de l'ICT. Toute association reconnue se voit attribuer une adresse électronique sous la forme nomassociation@ict- toulouse.fr. Cette adresse constitue une liste de diffusion des membres du bureau de l'association. La gestion des abonnés est assurée par l'association elle-même. Toute association reconnue pourra faire diffuser, via le service Vie Etudiante de l'ICT, des messages électroniques ayant pour objet la promotion de projets soutenus par l'université.

ATTRIBUTION D'AIDES FINANCIERES

Les associations peuvent bénéficier de l'octroi d'aides financières annuelles de la part de l'ICT pour leur fonctionnement. Un dossier de demande d'aide financière est à constituer et à adresser au bureau de la Vie Etudiante (BVE). Les associations bénéficiaires d'une aide financière doivent justifier a posteriori de leur emploi par la production d'un bilan moral et financier de l'action. Cette justification conditionne le renouvellement éventuel de l'aide.

SERVICES POUR LES APPRENANTS

Les apprenants peuvent participer aux activités organisées par la Vie Etudiante, l'Engagement solidaire, l 'Aumônerie, la Vie Culturelle. Ils ont accès au SOIE. Les locaux du Foyer étudiant, des espaces de travail partagés, de la salle Saint Dominique, le Café de l'ICT sont à leur disposition (cf. règlement intérieur de ces lieux le cas échéant).