institut
de **travail social**
de la région auvergne

LIVRET D'ACCUEIL #2

2020-2021

Informations pratiques

La Région Auvergne-Rhône-Alpes

ISO 9001 BUREAU VERITAS Certification

Datadock

V1 du 01/09/2020

SOMMAIRE

1. LES SALLES DISPONIBLES

L'ITSRA s'étend sur près de 6 000 m² et comprend 33 salles de cours (de 6 à 60 places) réparties sur 5 niveaux dont :

- 2 amphis modulables de 125 places équipés en vidéo projection et son
- 8 salles équipées en vidéo projection
- 2 salles de manutention (lits médicalisés, lève-personne, fauteuils roulants)
- 1 cuisine pédagogique
- 1 Centre de Ressources Documentaires avec plus de 50000 références et accès Wifi (CRD)
- 1 salle de visionnage (fond d'archive de 2500 films documentaires)
- 1 salle (la « pause ») dédiée à la lecture
- 1 salle de recherche documentaire (internet)
- 1 salle bureautique au CRD
- 1 salle informatique
- 1 espace cafétéria équipé de fours à micro-ondes et de réfrigérateurs

2. LE CENTRE DE RESSOURCES DOCUMENTAIRES

Le Centre de Ressources Documentaires propose :

A distance	Accès à la base de données, Réservation d'ouvrages, Accès compte lecteur, Articles de revues & ouvrages en ligne Rapports, Textes juridiques, Documents audio, Annuaires des établissements sanitaires, sociaux et médico-sociaux, Information dans la presse en lien avec le secteur.
Sur place **De 8h30 à 17h30**	Accès à la base de données, Ouvrages, Bandes dessinées, Guides et dictionnaires spécialisés, Revues spécialisées, Ecrits d'étudiants, Documents audiovisuels.

Les bases de données concernent de nombreux domaines, tels que l'animation, l'anthropologie, la démographie, le droit, l'économie, l'éducation, l'éthique, l'ethnologie, la gérontologie, le handicap, l'histoire des idées, l'adaptation, le management, la pédagogie, la petite enfance, la philosophie, la politique sociale, la pratique d'intervention sociale, la psychanalyse, la psychiatrie, la psychologie, la psychologie sociale, la santé, la sociologie, la technique éducative, …

Au total, c'est plus de 50 000 références, actualisées quotidiennement et interrogeables à distance sur itsra.bibli.fr.

Les conditions de prêt :

Il est possible aux adhérents d'emprunter un maximum de **6 livres et/ou écrits d'étudiants** (durée de l'emprunt : 1 mois), les autres documents sont à consulter sur place.

La réservation de documents est possible sur place, ou à distance (1 seule réservation) sous réserve que le document ne soit pas disponible dans les rayons.

Formation à la recherche documentaire :

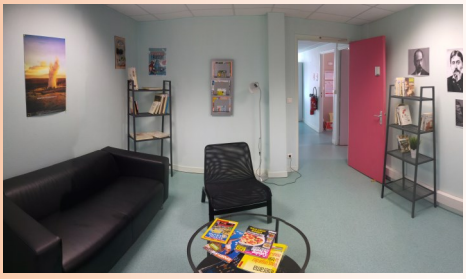
Toutes les promotions entrantes à l'ITSRA bénéficient d'une formation avec les documentalistes : présentation des services disponibles au CRD, travaux pratiques sur l'utilisation de la base de données.

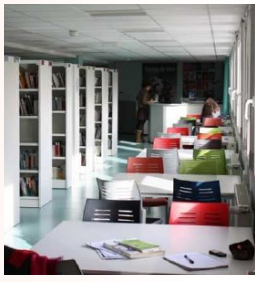
Le CRD est ouvert aux apprenants après versement d'une caution de 100€.

Accès au CRD	Adhésion	Caution
Apprenants et intervenants	Gratuit	100€
Etudiant extérieur	15€	100€
Salarié extérieur	30€	100€
Demandeur d'emploi	Gratuit sur présentation d'un justificatif	100€

"La Pause"

Cet espace de lecture, en dehors du travail social, vous accueille et vous propose : revues, livres (poésie, romans, théâtre, arts, BD, …), littérature jeunesse, et des sélections documentaires sur des thèmes d'actualité le temps d'une pause.

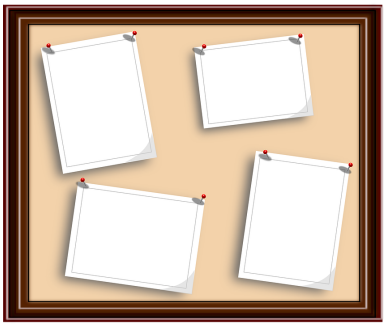




3. LES PANNEAUX D'AFFICHAGE

Plusieurs panneaux d'affichage sont présents à chaque étage de l'institut permettant aux apprenants et aux différents services de l'institut de faire part de diverses informations :

- Des panneaux dédiés aux affichages des apprenants (au rez-de-chaussée et gérés par les apprenants),
- Des panneaux dédiés aux offres d'emplois (au rez-de-chaussée et gérés par l'accueil),
- Des panneaux dédiés aux différentes filières (à tous les étages et gérés par les coordonnateurs),
- Des panneaux dédiés à l'administration (à tous les étages et gérés par l'administration).



4. LA RESTAURATION SUR PLACE

Au rez-de-chaussée, vous disposez d'un espace aménagé (mise à disposition de tables, chaises, réfrigérateurs, micro-ondes, coin lavabo, machine à sandwichs) pour prendre votre repas sur place.

Bonnes pratiques :

Libérez votre place dès que vous avez terminé de prendre votre repas.

Ne pas manger dans les salles de cours.

5. LES CONSIGNES DE SÉCURITÉ

Dès l'audition du signal d'évacuation :

Fermez les fenêtres → Eteignez les lumières et coupez les énergies (ordinateurs, …) → Fermez les portes

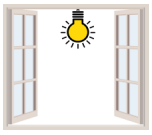
Evacuez dans le calme → Ne revenez jamais en arrière → Rejoignez le point de rassemblement

Consignes d'utilisation des salles de cours :

L'utilisation des cafetières et bouilloires est interdite dans les salles de cours par respect des consignes de sécurité.
Leur utilisation n'est autorisée que dans la cafétéria.

Il est strictement interdit de manger dans les salles de cours.

Les tables et chaises doivent être remises en place à la fin du cours.
Voir le plan affiché dans la salle.



Veillez à ce que les fenêtres soient fermées et que les lumières soient éteintes lorsque que vous quittez la salle.

6. LA CHARTE INTERNET

Introduction

Le contexte et les enjeux :
Les différents outils technologiques utilisés offrent aux apprenants de l'ITSRA une grande ouverture vers l'extérieur. Cette ouverture peut apporter des améliorations importantes de la performance si l'utilisation de ces outils technologiques est faite à bon escient et selon certaines règles.

A l'inverse, une mauvaise utilisation de ces outils peut avoir des conséquences graves. En effet, ils augmentent les risques d'atteinte à la confidentialité, d'atteinte à l'intégrité et à la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vols de données).

La Loi, les textes réglementaires et la présente charte définissent les droits et obligations des personnes utilisant les ressources informatiques.

La présente charte informatique est un code de déontologie formalisant les règles légales et de sécurité relatives à l'utilisation de tout système d'information et de communication au sein de l'ITSRA.

Le champ d'application :
La présente charte s'applique à l'ensemble des apprenants. Dès l'entrée en vigueur de la présente charte, chaque apprenant de l'ITSRA en recevra un exemplaire. Il devra en prendre connaissance, la retourner signer et s'engager à la respecter.

L'objectif :

Les règles générales d'utilisation

Les utilisateurs sont supposés adopter un comportement responsable s'interdisant par exemple toute tentative d'accès à des données ou à des sites qui leurs seraient interdits.
Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques, ainsi que du contenu de ce qu'il affiche, télécharge ou envoie et s'engage à ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau.

Les droits et les devoirs des utilisateurs :

L'accès aux ressources est règlementé. Toute personne étudiant à l'ITSRA dispose d'un droit d'accès aux postes informatiques. Ce droit d'accès est :

- Strictement personnel.
- Incessible.

Les ressources matérielles et logicielles mises à disposition constituent un outil de travail nécessaire. Chaque utilisateur doit adopter une attitude responsable et respecter les règles définies sur l'utilisation des ressources et notamment :

- Respecter l'intégrité et la confidentialité des données.
- Ne pas perturber la disponibilité du système d'information.
- Ne pas stocker ou transmettre d'informations portant atteinte à la dignité humaine.
- Ne pas marquer les données exploitées d'annotations pouvant porter atteinte à la dignité humaine ou à la vie privée ou aux droits et images de chacun ou faisant référence à une quelconque appartenance à une ethnie, religion, race ou nation déterminée (loi « informatique et liberté » du 06/01/1978).
- Respecter le droit de propriété intellectuelle : non reproduction et/ou non diffusion de données soumises à un droit de copie non-détenu, interdiction de copie de logiciel sans licence d'utilisation.
- Ne pas porter atteinte à la sécurité du système d'information par l'utilisation de "ressources extérieures" matérielles ou logicielles.
- Respecter les contraintes liées à la maintenance du système d'information.

Les droits et devoirs de l'ITSRA :

L'ITSRA s'engage à :

- Mettre à disposition les ressources informatiques matérielles et logicielles nécessaires au bon déroulement de la mission des utilisateurs.
- Mettre en place des programmes de formation adaptés et nécessaires aux utilisateurs pour une bonne utilisation des outils.
- Informer les utilisateurs des diverses contraintes d'exploitation (interruption de service, maintenance, modification de ressources,) du système d'information susceptibles d'occasionner une perturbation.
- Effectuer les mises à jour nécessaires des matériels et des logiciels composant le système d'information afin de maintenir le niveau de sécurité en vigueur dans le respect des règles d'achat et des budgets alloués.
- Respecter la confidentialité des "données utilisateurs" auxquelles il pourrait être amené à accéder pour diagnostiquer ou corriger un problème spécifique.

Politique de confidentialité

Les informations recueillies vous concernant font l'objet d'un traitement destiné à l'ITSRA.
Sa finalité est la gestion de votre dossier apprenant.
Les destinataires de ces données sont le personnel de l'ITSRA ainsi qu'à des fins statistiques les autorités de tutelles de l'ITSRA. La durée de conservation des données est de 10 ans.

Vous bénéficiez d'un droit d'accès, de rectification, de portabilité, d'effacement de celles-ci ou une limitation du traitement.

Vous pouvez, sous réserve de la production d'un justificatif d'identité valide, vous opposer au traitement des données vous concernant et disposez du droit de retirer votre consentement à tout moment en vous adressant à la direction de l'ITSRA.
En cas de demande de suppression complète de vos données, l'ITSRA considérera que vous êtes définitivement démissionnaire.
Vous avez la possibilité d'introduire une réclamation auprès d'une autorité de contrôle.

L'analyse et le contrôle

Pour des nécessités de sécurité, de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent, sous le contrôle du responsable informatique, être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi relative à l'informatique, aux fichiers et aux libertés.

Les sanctions

En cas de violation de la charte, l'établissement pourra suspendre immédiatement les droits d'accès de l'utilisateur aux ressources informatiques. Cette décision interviendra une fois que l'utilisateur aura été entendu. L'intéressé pourra être passible d'une sanction disciplinaire.

L'établissement étant tenu par la loi de signaler toute violation constatée des lois, l'utilisateur s'expose à des sanctions pénales prévues par les lois en vigueur.

Les postes informatiques

Un ensemble "matériels - système d'exploitation - logiciels" est mis à disposition des utilisateurs :

Matériel : unité centrale, écran, clavier, souris, ...

Système d'exploitation : Windows, …

Logiciels : pack bureautique, logiciels de communication, logiciels de gestion, applications spécifiques.

Le matériel informatique est fragile, il faut en prendre soin.
Toute installation logicielle est placée sous la responsabilité du Responsable informatique.

En cas d'absence momentanée, l'utilisateur doit verrouiller sa session.

En cas d'absence prolongée, l'utilisateur doit quitter les applications et verrouiller sa session.

À la fin de la journée, l'utilisateur doit quitter les applications, arrêter le système par l'arrêt du logiciel, éteindre l'écran et l'imprimante.

Un premier niveau de sécurité consiste à utiliser des mots de passe sûrs non communiqués à des tiers et régulièrement modifiés.

L'utilisateur doit signaler tout dysfonctionnement ou anomalie au Responsable informatique.

Les supports amovibles (CD, clé USB, etc.) provenant de l'extérieur doivent être soumis à un contrôle antivirus préalable.

Les sites internet

L'utilisation d'Internet est réservée à des fins pédagogiques.
L'utilisateur s'engage lors de ses consultations Internet à ne pas se rendre sur des sites portant atteinte à la dignité humaine (pédopornographie, apologie des crimes contre l'humanité et provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non à une ethnie, une nation, une race ou une religion déterminée).

Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.

Le stockage permanent sur les postes de données téléchargées sur Internet est interdit.

Le stockage sur le réseau de données à caractère non professionnel téléchargées sur Internet est interdit.

Les réseaux sociaux

L'utilisation doit être appropriée et doit respecter le devoir de réserve.
Les conditions d'utilisation et d'accès sont définies (restrictions et limites pratiques).

Annexe, les bases légales

Cette présente partie a pour objectif d'informer les utilisateurs des textes législatifs et réglementaires dans le domaine de la sécurité des systèmes d'information.

La Réglementation :

Loi n° 78-17 du 06/01/1978 sur l'informatique, les fichiers, les libertés.
Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'informatique.

Loi n° 85-660 du 03/07/1985 sur les droits d'auteur et a protection des logiciels.
Elle interdit à l'utilisateur d'un logiciel toute reproduction de celui-ci autre que l'établissement d'une copie de sauvegarde.

Loi n° 88-19 du 05/01/1988 relative à la fraude informatique.
Cette loi, dite de GODEFRAIN, vise à lutter contre la fraude informatique en réprimant :

- Les accès ou maintien frauduleux dans un système d'information,
- Les atteintes accidentelles ou volontaires au fonctionnement,
- La falsification des documents informatiques et leur usage illicite,
- L'association ou l'entente en vue de commettre un de ces délits.

Loi n° 91-643 du 10/07/1991 relative au secret des correspondances émises par voie de télécommunication.

Loi n° 2000-230 du 13/03/2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Loi n° 2004-575 du 21/06/2004 pour la confiance dans l'économie numérique.
Elle est destinée à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires aussi bien techniques que commerciaux.

Loi n° 2012-410 du 27/03/2012 relative à la protection de l'identité.

Le règlement no 2016/679, dit règlement général sur la protection des données (RGPD, ou encore GDPR, de l'anglais General Data Protection Regulation), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.
Après quatre années de négociations législatives, ce règlement a été définitivement adopté par le Parlement européen le 14 avril 2016. Ses dispositions sont directement applicables dans l'ensemble des 28 États membres de l'Union européenne à compter du 25 mai 2018.
Ce règlement remplace la directive sur la protection des données personnelles adoptée en 1995 (article 94 du règlement) ; contrairement aux directives, les règlements n'impliquent pas que les États membres adoptent une loi de transposition pour être applicables.
Les principaux objectifs du RGPD sont d'accroître à la fois la protection des personnes concernées par un traitement de leurs données à caractère personnel et la responsabilisation des acteurs de ce traitement. Ces principes pourront être appliqués grâce à l'augmentation du pouvoir des autorités de régulation.

Le Code Pénal :

Code Pénal Livre 3 Titre 2 Chapitre III : Des atteintes aux systèmes de traitement automatisé de données.

- **Article 323-1 :**

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30.000 euros d'amende. »

- **Article 323-2 :**

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75.000 euros d'amende. »

- **Article 323-3 :**

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75.000 euros d'amende. »

- **Article 323-4 :**

« La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

- **Article 323-5 :**

« Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26.
2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise.
3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.
4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés.»
5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics.
6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés.

7º L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35. »

- **Article 323-6 :**

« Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre. Les peines encourues par les personnes morales sont :
1º L'amende, suivant les modalités prévues par l'article 131-38.
2º Les peines mentionnées à l'article 131-39.
L'interdiction mentionnée au 2º de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. »

- **Article 323-7 :**

« La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines. »

Cette charte est en cours de validation par le Conseil d'Administration.

7. L'ACCÈS WI-FI

Le centre de ressources documentaires est équipé de postes informatiques destinés aux apprenants mais il est possible de travailler avec votre propre matériel.

Vous avez accès au WI-FI dans l'ensemble du bâtiment (salles de cours, CRD, cafétéria...)

Comment se connecter au Wi-Fi ?

Une adresse mail spécifique vous sera communiquée après votre arrivée dans l'établissement. Cette adresse vous permettra de vous connecter au réseau Wifi et d'accéder aux fonctionnalités d'Office 365.

Avant de vous connecter, merci de prendre connaissance de la Charte d'utilisation du matériel informatique et du service Hotspot de l'ITSRA :

L'utilisation du matériel informatique et du service Hotspot de l'ITSRA est soumis en premier lieu, au respect des lois et des règlements en vigueur.

L'utilisation de ce service vaut acceptation irréfragable par l'utilisateur, sans qu'aucune signature ne soit nécessaire, de l'ensemble des dispositions et obligations contenues dans la présente Charte.

L'utilisation du service Hotspot de l'ITSRA permettant l'accès à Internet est autorisée pendant les heures d'ouverture de l'établissement.

L'utilisateur reconnaît être dans un lieu ouvert au public. Il s'engage à utiliser son matériel informatique, (portable, assistant personnel ou tout autre matériel Wi-Fi) et ce service, d'une manière conforme à la loi et à la net étiquette en s'interdisant notamment tout comportement et tout usage contraire à l'ordre public et aux bonnes mœurs.

⇒ En particulier il ne devra pas utiliser son matériel ou ce service à des fins illégales, illicites, interdites, c'est-à-dire, sans que cette liste ait un caractère exhaustif :

- Il s'engage à respecter la loi et s'interdit d'accéder, de mettre en ligne ou d'afficher des contenus et informations, provenant ou non d'une mise en ligne sur le réseau Internet mais considérés comme illégaux par les textes ou les tribunaux tels, les informations, messages, textes, images ou vidéos ayant un caractère violent, d'incitation à la violence ou à la haine, dégradant pour la personne humaine, pornographique ou pédophile et/ou ayant un caractère provocant et portant atteinte à l'intégrité ou à la sensibilité des utilisateurs du réseau et/ou des consommateurs et usagers de l'établissement.

- A titre d'information, il est précisé que l'accès Wi-Fi de l'ITSRA est sécurisé par un outil de filtrage systématique de type « contrôle parental » et, en conséquence, l'utilisateur est informé que certains sites sont inaccessibles.

⇒ **L'utilisateur s'engage à respecter la vie privée** de toute personne et le secret des correspondances, il s'interdit d'intercepter tout message et communication émis par la voie des télécommunications.

⇒ **Il s'engage à respecter la législation sur les données personnelles et les traitements automatisés d'informations nominatives ainsi que la législation et les textes relatifs aux droits d'auteur, marques, brevets, à la propriété intellectuelle et industrielle.** Il s'interdit toute reproduction ou usage en infraction de ces législations, qu'il s'agisse de créations multimédia, de logiciels, de textes, d'articles de presse, de photos, de sons, d'images de toute nature, de marques, de brevets, de dessins et modèles, étant précisé que toute mention relative à l'existence de droits sur ces éléments et/ou données et/ou fichiers ne peuvent faire l'objet d'une suppression et que toute reproduction d'une œuvre ou de l'un de ces éléments et/ou fichiers et/ou données sans consentement du titulaire des droits constitue une contrefaçon.

⇒ Dans le cadre de l'usage du service Hotspot de l'ITSRA, l'utilisateur s'interdit de :

- récolter ou collecter toute information concernant des tiers sans leur consentement ;
- diffamer, diffuser, harceler, traquer, menacer quiconque, ni violer les droits d'autrui ;
- créer une fausse identité ;
- tenter d'obtenir un accès non autorisé à un service et/ou à un fichier, ou une donnée ;
- diffuser ou télécharger des éléments contenant des logiciels ou autres éléments protégés par les droits de propriété intellectuelle, à moins qu'il ne détienne lesdits droits ou qu'il ait reçu toutes les autorisations nécessaires pour le faire ;
- d'adresser tout message indésirable ni d'effectuer des envois de type « spamming » ;
- d'adresser tout courrier et/ou message électronique comprenant des propos menaçants, injurieux, diffamatoires, obscènes, indécents, illicites ou portant atteinte aux droits des personnes et à la protection des mineurs ;
- transmettre tout virus, cheval de Troie, bombe logique ou tout autre programme nuisible ou destructeur pour les tiers et/ou tout utilisateur ;
- tenter d'obtenir un accès non autorisé à un système automatisé de traitement de données et s'y maintenir ;
- perturber les services et/ou contenus et/ou données auxquels il accède ;
- d'envoyer des chaînes de lettres ou proposer des ventes dites « boule de neige » ou pyramidales ;
- d'adresser toute publicité, message promotionnel ou toute autre forme de sollicitation ou démarchage non sollicité.

⇒ L'utilisateur reconnaît avoir reçu toute information nécessaire aux spécifications et modalités d'utilisation du service Hotspot de l'ITSRA, laquelle met en œuvre un logiciel de protection automatique à l'effet de sélectionner ou restreindre l'accès à certains sites, serveurs ou données.

⇒ Il appartient à l'utilisateur de vérifier qu'il dispose des équipements matériels, logiciels, navigateurs lui permettant d'utiliser ce service. L'ITSRA n'est en aucun cas responsable des équipements choisis sous la responsabilité de l'utilisateur, lequel reste seul responsable de leur sécurité et de leur protection.

⇒ L'ITSRA, à la demande de toute autorité administrative ou judiciaire compétente, ou si elle l'estime nécessaire, pourra suspendre temporairement ou définitivement toute utilisation du service sans que sa responsabilité ne puisse être recherchée et sans que l'utilisateur ne puisse revendiquer une quelconque indemnisation ou réparation.

⇒ L'ITSRA ne peut être en aucun cas tenu de réparer les préjudices directs et/ou indirects subis du fait de l'utilisation du service WI-FI par l'utilisateur, ce dernier étant sous la responsabilité des utilisateurs dans le respect de la présente Charte. L'utilisateur reconnaît que l'ITSRA ne peut être responsable des contenus ou services auxquels il accède et ne garantit ni l'accessibilité aux contenus et services ni la rapidité d'utilisation, l'accès au service WIFI pouvant être suspendu à tout moment sans préavis.

⇒ L'ITSRA informe les utilisateurs du service que les nouvelles dispositions applicables en matière de lutte contre le terrorisme impliquent l'obligation de conserver pendant une durée de 12 mois les données techniques de connexion, à savoir : "utilisateur", adresse MAC, heure, durée et lieu d'origine des communications à l'exception de leur contenu.

⇒ Afin de profiter pleinement du service Hotspot, l'ITSRA conseille à tous les utilisateurs de veiller à leurs matériels informatiques en s'assurant que les ordinateurs portables et assistants personnels ne soient pas laissés sans surveillance, en faisant attention aux consommations qui pourraient endommager leurs matériels et en s'assurant de posséder un antivirus à jour.

institut
de **travail social**
de la région auvergne