

## FICHE PRATIQUE

RESSOURCES HUMAINES ▶ COMPÉTENCES PERSONNELLES ▶ LEADERSHIP POSITIF

# Confidentialité : Faculté de gérer les informations sensibles avec discrétion et respect

Ce document est régulièrement mis à jour.

Téléchargez gratuitement la dernière version sur <u>Débloque-tes-soft-skills.com</u>

#### MISE EN GARDE

Pour la plupart d'entre nous, les Soft Skills apprises en formation, sur la base d'une liste de recettes à appliquer dans telle ou telle situation, ne sont pas durablement exploitables : les mauvais comportements reprennent très vite le dessus, la Soft Skill ne peut pas s'exprimer, elle est BLOQUÉE par un ensemble de comportements contre-productifs dont on ne sait pas se débarrasser.

Suite à la découverte d'un incroyable protocole imaginé par 2 professeurs de la Harvard Business School, une offre exclusive permet désormais de DÉBLOQUER réellement et définitivement ses Soft Skills.

Découvrez cette offre sur <u>Débloque-tes-soft-skills.com</u>

Le contenu de cette fiche pratique a été généré par une Intelligence Artificielle pilotée par une Intelligence Humaine



## Comportements recommandés :

## 1. Ne partager les informations sensibles qu'avec les personnes autorisées

→ Toute donnée RH doit être traitée avec précaution et uniquement par les parties concernées.

Exemple : « Je ne transmets les informations salariales d'un employé qu'à son manager direct et au service comptable. »

## 2. Utiliser des outils sécurisés pour stocker et partager les données sensibles

→ Un bon usage des technologies garantit la protection des informations.

Exemple : « J'enregistre les contrats et dossiers du personnel dans un logiciel RH sécurisé et non sur mon ordinateur personnel. »

## 3. Verrouiller ses fichiers et documents contenant des données confidentielles

→ Éviter les fuites accidentelles en sécurisant l'accès aux informations.

Exemple : « J'utilise un mot de passe pour accéder aux dossiers contenant des informations confidentielles. »

## 4. Éviter de discuter d'informations sensibles dans des lieux publics ou ouverts

→ Le respect de la confidentialité implique de choisir un environnement approprié pour échanger.

Exemple : « Je ne parle pas d'un licenciement en cours à la machine à café où d'autres collègues peuvent entendre. »

# 5. S'assurer que les documents papier contenant des informations confidentielles sont bien rangés ou détruits

→ Un bon archivage évite la divulgation accidentelle.

Exemple : « Je ne laisse pas traîner des fiches de paie sur mon bureau et je les range dans une armoire fermée à clé. »

## 6. Ne pas envoyer d'informations sensibles par email sans précaution

→ Certains échanges nécessitent un cadre plus sécurisé.

Exemple : « J'envoie un fichier contenant des données personnelles uniquement



via un canal crypté et sécurisé. »

## 7. Informer les collaborateurs de la confidentialité des informations échangées

→ Sensibiliser à la protection des données aide à instaurer une culture du respect de la vie privée.

Exemple : « Avant de partager des informations en réunion, je rappelle que ces données ne doivent pas être divulguées en dehors du cadre professionnel. »

### 8. Ne pas céder aux pressions pour divulguer des informations confidentielles

→ Un collaborateur RH doit être ferme et éthique.

Exemple : « Un collègue insiste pour connaître le salaire d'un autre employé, je refuse fermement et lui rappelle les règles de confidentialité. »

## S'assurer que toute impression de documents confidentiels est bien récupérée immédiatement

→ Éviter que des documents sensibles restent accessibles à d'autres.

Exemple : « Je récupère immédiatement mes impressions de contrats de travail pour éviter qu'elles restent visibles sur l'imprimante commune. »

# 10. Respecter le cadre légal et réglementaire lié à la protection des données personnelles

→ Un RH doit toujours agir dans le respect des lois en vigueur (ex: RGPD).

Exemple : « Avant de collecter et stocker certaines données personnelles, je m'assure que nous avons bien le consentement du salarié. »

## Comportements à éviter :

## 1. Divulguer des informations confidentielles à des collègues non concernés

→ Partager des données sans raison peut avoir des conséquences graves.

Exemple : « Je parle du salaire d'un employé à un collègue qui n'a pas à en être



informé. »

#### 2. Laisser des documents sensibles accessibles à tout le monde

→ Un manque de précaution peut entraîner des fuites d'informations.

Exemple : « Je laisse des dossiers de paie sur mon bureau au lieu de les ranger dans une armoire sécurisée. »

## 3. Utiliser des plateformes non sécurisées pour stocker des données RH

→ Un risque majeur pour la sécurité des informations.

Exemple : « J'enregistre des fichiers RH sensibles sur mon Google Drive personnel au lieu d'utiliser l'outil sécurisé de l'entreprise. »

## 4. Parler de sujets confidentiels dans des endroits inappropriés

→ Les discussions sensibles doivent rester privées.

Exemple : « Je discute d'un licenciement à venir dans un open space où plusieurs collègues peuvent entendre. »

### 5. Envoyer des emails contenant des informations sensibles sans protection

→ Une mauvaise gestion des emails peut entraı̂ner des fuites.

Exemple : « J'envoie la liste des augmentations de salaire à un mauvais destinataire par erreur. »

### 6. Ne pas sensibiliser les collaborateurs à l'importance de la confidentialité

→ Il faut rappeler régulièrement les bonnes pratiques à adopter.

Exemple : « Je ne dis rien lorsqu'un manager parle d'une évaluation de performance confidentielle devant d'autres employés. »

### 7. Ne pas sécuriser son ordinateur ou ses accès aux logiciels RH

→ Laisser un accès libre aux données sensibles est une faille de sécurité.

Exemple : « Je quitte mon poste sans verrouiller mon ordinateur alors que mon écran affiche des informations confidentielles. »

## 8. Céder aux pressions pour divulguer des informations

→ Une éthique irréprochable est essentielle en RH.



Exemple : « Un responsable me demande les motifs de l'arrêt maladie d'un salarié, je lui donne les détails alors qu'il n'y est pas autorisé. »

# Garder des fichiers contenant des informations confidentielles au-delà de la durée légale

→ Le respect du cycle de vie des données est crucial.

Exemple : « Je conserve des dossiers d'anciens salariés bien après leur départ, sans raison valable. »

# 10. Partager involontairement des informations sensibles sur les réseaux sociaux ou en dehors du cadre professionnel

→ Un manque de vigilance peut exposer l'entreprise à des risques.

Exemple : « Je mentionne sur LinkedIn que l'entreprise prépare un plan de licenciement avant que l'annonce ne soit officielle. »

#### Conclusion

Le respect de la confidentialité en RH est un impératif absolu. Une gestion rigoureuse et éthique des informations sensibles protège les collaborateurs et renforce la confiance au sein de l'entreprise. En appliquant les bonnes pratiques et en évitant les erreurs courantes, un professionnel des RH assure une gestion sécurisée et conforme aux obligations légales.