Utiliser Claude au travail sans risque : 9 interdits et 9 bonnes pratiques

Réglages de confidentialité, données à ne jamais coller, anonymisation, connecteurs : le guide en 9 interdits et 9 bonnes pratiques pour utiliser Claude au travail.

BLYX-AGENCY.COM · 5 NOVEMBRE 2026 · PAR PIERRE CORDELIER

Dans beaucoup d'entreprises, des salariés utilisent leur compte Claude personnel pour travailler. Ils collent un mail client, un tableur, un bout de code, et gagnent une heure. Personne ne leur a dit où était la limite.

Ce n'est pas un problème d'outil, c'est un problème de règles. En 2023, trois fuites de données chez Samsung vers ChatGPT en vingt jours ont conduit l'entreprise à interdire temporairement ces outils sur ses appareils. Claude fonctionne autrement, mais la question est la même : qu'est-ce qui quitte l'entreprise quand on appuie sur Entrée ?

Ce guide répond en 9 interdits et 9 bonnes pratiques, avec les réglages à faire, des prompts à copier et une règle d'équipe prête à adapter. Les durées de conservation citées sont celles des pages officielles d'Anthropic au 1er novembre 2026. Ces règles ont déjà changé en 2025 : vérifiez-les de temps en temps.

D'abord : de quel Claude parle-t-on ?

Tout ce qui suit vise le Claude personnel (Free, Pro, Max) utilisé po travail. Un plan Team ou Enterprise de l'entreprise est un autre cadre.

	Compte personnel (Free, Pro, Max)	Plan Team ou Enterprise
Entraînement sur vos conversations	Selon le réglage « Aider à améliorer nos modèles d'IA »	Pas d'entraînement sur votre contenu par défaut (page des tarifs)
Qui est responsable des données	Vous, sous les conditions grand public	L'entreprise cliente, sous les conditions commerciales
Réglages des connecteurs pour l'équipe	Chacun les siens	Le propriétaire peut régler chaque outil sur « Always allow », « Needs approval » ou « Blocked »

Les prix de Team sont affichés en dollars sur la page officielle (20 $ par siège et par mois en facturation annuelle, 25 $ en mensuel, au moment de notre recherche, sans date sur la page). Vérifiez avant de budgéter.

Les 9 interdits

Pour chacun : ce qu'il ne faut pas faire, pourquoi, et ce qu'on fait à la place.

Interdit 1. Laisser l'entraînement activé sur un compte utilisé pour le travail

Réglage activé, vos conversations nouvelles ou reprises peuvent être conservées, sous forme dépersonnalisée, jusqu'à 5 ans dans les pipelines d'entraînement. Réglage désactivé, Anthropic n'utilise plus vos chats pour entraîner ses futurs modèles. Deux nuances : les modèl déjà entraînés gardent ce qui leur a déjà été envoyé, et les

conversations signalées par les classificateurs de sécurité peuvent [illegible] à la sécurité.

À la place : Paramètres, Confidentialité, désactivez « Aider à améliorer nos modèles d'IA ». Sur mobile, passez par votre nom, puis Paramètres.

Interdit 2. Coller du code source « juste pour trouver le bug »

C'est l'erreur la plus citée. À l'origine du cas Samsung, des ingénieurs avaient collé du code source et des notes de réunion dans ChatGPT. Le code d'une entreprise est un actif : sa copie dans un outil tiers n'est pas anodine.

À la place : décrivez le comportement du bug, collez trois lignes isolées et rendues génériques, ou utilisez l'outil validé par l'entreprise.

Interdit 3. Coller des données personnelles de clients ou de collègues

Noms, e-mails, téléphones, numéros de dossier. Si ces données sont sur votre compte personnel, elles sortent du cadre de l'entreprise. C'est un sujet RGPD pour la boîte, pas seulement pour vous.

À la place : anonymisez d'abord (bonne pratique 4), ou passez par l'outil de l'entreprise.

Interdit 4. Coller des identifiants, mots de passe ou clés d'accès

Les pages d'aide de Claude déconseillent elles-mêmes de saisir mo[illegible] de passe et données financières. Une clé collée dans une conversa[illegible] est une clé à changer.

À la place : jamais, pas une seule fois. Si c'est arrivé, changez la clé tout de suite.

Interdit 5. Coller ce qui n'est pas public : projets, marges, contrats

Roadmaps, prévisions, grilles de prix, marges, contrats, tout ce qui est sous NDA ou pas encore annoncé. Votre client ou votre partenaire ne vous a pas autorisé à le transmettre à un tiers.

À la place : demandez l'aide de Claude sur la structure (« comment présenter une grille de prix en trois niveaux ? »), pas avec vos vrais chiffres.

Interdit 6. Importer le fichier d'origine

Un PDF ou un tableur peut contenir bien plus que ce que vous voyez : auteur, commentaires, historique des modifications, colonnes ou feuilles masquées. Ce point relève de la connaissance générale des formats Office et PDF et non d'une page d'Anthropic : le plus simple est de le vérifier vous-même en ouvrant les propriétés d'un fichier test.

À la place : copiez le seul passage utile dans la conversation, pas le fichier.

Interdit 7. Connecter votre messagerie pro à votre Claude personnel

Un connecteur Gmail ou Microsoft 365 donne à Claude vos droits dans ce service : il peut lire ce que vous lisez. Les mails de toute l'entreprise, ceux de vos clients, passent alors par un compte qui n'est pas celu[illegible] l'entreprise, sous les conditions grand public.

À la place : si vous avez besoin de cette fonction, elle se déploie sur un plan Team ou Enterprise, où l'entreprise la règle.

Interdit 8. Connecter « tout mon Drive » par confort

C'est la même logique, avec des documents. Plus l'accès est large, plus la quantité exposée est grande, et vous ne vous souvenez plus de ce que contient ce vieux dossier.

À la place : le minimum. Un seul dossier, ou le passage collé à la main. Si vous pouvez coller la chose utile, vous n'avez pas besoin du connecteur.

Interdit 9. Installer des connecteurs inconnus

Les connecteurs prêts à l'emploi (Slack, Google Drive, GitHub, Gmail, Google Agenda, Microsoft 365, Linear) viennent d'une liste connue. Les connecteurs personnalisés, eux, peuvent relier Claude à des services qu'Anthropic n'a pas vérifiés. La politique de l'annuaire le dit : le comportement d'un outil peut changer sans prévenir, et l'on doit se connecter uniquement à des organisations de confiance.

À la place : préférez les connecteurs de l'annuaire, et pour un connecteur personnalisé, n'installez que celui d'une organisation que vous connaissez.

Les 9 bonnes pratiques

Bonne pratique 1. Désactiver l'entraînement, dès aujourd'hui

C'est le premier réflexe, il prend trente secondes (voir l'interdit 1). Sans abonnement d'entraînement, la conservation annoncée par Anthropic en août 2025 est de 30 jours. Les retours « pouce haut » ou « pouce bas » et les signalements de bug sont conservés 5 ans, quel que soit le réglage : n'y écrivez rien de confidentiel.

Bonne pratique 2. Faire payer l'entreprise

Le vrai remède n'est pas de bricoler des précautions sur un compte perso. C'est d'avoir un outil de l'entreprise. Le plan Team ou Enterprise ne s'entraîne pas sur votre contenu par défaut, et l'entreprise y est le responsable des données. Demandez-le à votre direction. Si vous êtes la direction : le déployer dans l'équipe est la décision la plus rentable de ce guide. Notre guide Déployer Claude Team dans votre équipe en 5 jours détaille la méthode.

Attention : un plan professionnel ne dispense pas de réfléchir. La conformité RGPD dépend du contrat et de l'usage, pas seulement de l'absence d'entraînement.

Bonne pratique 3. Faire le test de la diffusion interne

Avant de coller, posez-vous une question : « Est-ce que ça m'irait si ce texte circulait dans toute l'entreprise, avec mon nom dessus ? » Si la réponse est non, vous anonymisez ou vous ne collez pas.

Bonne pratique 4. Remplacer les noms par des rôles

« Marie Durand, directrice achats chez Fonderie Martin » devient « la directrice achats d'un fournisseur ». Un client devient « le client A ».

collègue « le manager ». Claude n'a pas besoin de savoir qui, il a besoin de la forme du problème.

Bonne pratique 5. Remplacer les chiffres par des chiffres du même ordre

Un chiffre d'affaires de 4,2 M€ devient 4 M€ ou 4,5 M€. Une marge de 31 % devient 30 %. Le raisonnement tient, l'information réelle reste chez vous.

Une limite à connaître : la CNIL distingue l'anonymisation, irréversible, de la pseudonymisation, réversible, dont les données « conservent un caractère personnel ». Remplacer un nom par « le client A » ne rend pas les données anonymes si quelqu'un peut recouper le reste (la ville, le montant, le poste). Anonymiser réduit le risque, pas à zéro.

Le prompt ci-dessous fait le travail pour vous. Lancez-le dans une conversation où vous collez le texte brut, ou mieux, utilisez-le sur un texte déjà réduit au strict nécessaire.

```
Voici un texte que je veux soumettre à une IA. Avant cela, prépare
une version anonymisée.
Règles :
1. Remplace chaque nom de personne par un rôle (« le client », « la
responsable RH »).
2. Remplace chaque nom d'entreprise par une description générique
(« un fournisseur de pièces »).
3. Remplace chaque chiffre par un chiffre du même ordre de
grandeur, jamais le chiffre réel.
4. Supprime les adresses, e-mails, téléphones, numéros de dossier
ou de contrat.
5. Signale-moi tout ce qui pourrait encore permettre de reconnaître
la personne ou l'entreprise (poste très rare, ville, événement
précis).
Rends-moi uniquement le texte anonymisé, puis la liste de ce que tu
```

```
as signalé. N'invente rien.
Texte : [coller ici]
```

Cette étape suppose que le texte brut est déjà dans une conversation : réservez-la à des contenus peu sensibles. Pour du contenu vraiment sensible, anonymisez à la main, ou dans l'outil de l'entreprise.

Bonne pratique 6. Ne copier que le passage utile

Trois paragraphes valent mieux qu'un document de quarante pages. Vous évitez les métadonnées cachées et vous obtenez une réponse plus précise.

Bonne pratique 7. Utiliser le mode Incognito pour un sujet sensible

Un chat incognito n'est pas enregistré dans l'historique ni dans la mémoire de Claude, et n'est pas utilisé pour l'entraînement, même si le réglage d'amélioration est activé. Pour l'ouvrir, cliquez sur l'icône fantôme en haut à droite d'un nouveau chat.

Ne dites pas qu'il « disparaît » à la fermeture. Il est conservé 30 jours par défaut pour la sécurité, et ne peut pas être rouvert une fois fermé. L'incognito protège de l'historique et de l'entraînement, pas de la conservation.

Bonne pratique 8. Régler les connecteurs au plus juste

Quand un connecteur est utile, appliquez trois règles :

1. Donnez le minimum de permissions que propose le connecteur.
2. Connectez le dossier ou l'espace utile, pas tout le service.

3. Sur Team ou Enterprise, le propriétaire règle chaque outil sur « Needs approval » pour que rien ne parte sans validation, ou « Blocked » pour ce qui ne doit pas servir. Ces réglages ne font que restreindre l'accès.

Rappelez-vous que les services connectés traitent les données chez eux, sous leurs propres conditions, parfois hors des États-Unis.

Bonne pratique 9. Faire le ménage chaque mois

Une fois par mois, dix minutes :

1. Dans Claude : Personnaliser, Connecteurs. Déconnectez ce qui ne sert pas.
2. Côté Google : ouvrez `myaccount.google.com/linkedapps` et retirez les applications dont vous ne vous servez plus. Retirer un accès n'efface pas la copie que l'application a déjà faite : il faut la demander au développeur.
3. Côté Microsoft : faites la même vérification dans les paramètres de votre compte. Nous n'avons pas vérifié le chemin exact, cherchez « applications autorisées » dans votre compte.

La fréquence mensuelle est un conseil, non une exigence de Google.

Deux sujets qui demandent une décision de l'entreprise

Deux points du quotidien ne se règlent pas avec un réglage.

Les données de santé et les données juridiques. Même anonymisées, elles sont les plus risquées. Ne les mettez pas dans

compte personnel. Un plan Team ou Enterprise ne s'entraîne pas sur votre contenu par défaut, mais à vous de vérifier, avec votre juriste, que le contrat et l'usage tiennent. Notre grille d'arbitrage IA et données juridiques vous aide à trancher.

Les projets personnels sur l'outil de l'entreprise. Si vous construisez un projet perso avec l'IA que l'entreprise paie, ou si vous utilisez votre IA perso sur le poste de travail, la question de la propriété se pose. Elle relève de votre contrat de travail et des conditions de l'outil : nous ne l'avons pas tranchée dans cette recherche. Clarifiez-la par écrit avec votre direction avant de commencer.

La règle d'équipe en cinq lignes

Si vous dirigez une PME, ne laissez pas chacun deviner. Voici une base à adapter, à afficher et à faire signer.

```
1. Les outils d'IA autorisés pour le travail sont : [liste]. Les
comptes personnels ne servent pas pour des données de l'entreprise.
2. Ne jamais saisir : identifiants et clés, données personnelles de
clients ou de salariés, code source, documents confidentiels ou
sous NDA.
3. En cas de doute, anonymiser : des rôles à la place des noms, des
chiffres du même ordre à la place des vrais.
4. Les connecteurs (messagerie, Drive, agenda) ne se branchent
qu'avec l'accord de [responsable], sur le minimum de périmètre.
5. Une erreur se signale tout de suite à [responsable] : le but est
de la corriger, pas de la cacher.
```

La dernière ligne compte. Un salarié qui craint une sanction cachera l'erreur, et vous perdrez le temps de réagir.

Le prompt pour auditer vos propres usages

Pour savoir où vous en êtes, demandez à Claude de vous poser les bonnes questions. Il ne voit pas vos réglages, mais il peut vous guider.

```
Je veux faire le point sur mon usage de Claude au travail. Pose-moi, une question à la fois, des questions sur : le type de compte que j'utilise (gratuit, Pro, Max, Team), les types de contenus que je colle ou importe, les connecteurs que j'ai branchés, mon réglage d'entraînement, mon usage de l'Incognito.
À la fin, donne-moi : 1) ce qui est à risque, classé du plus au moins grave, 2) trois actions à faire cette semaine, 3) ce que je dois demander à mon entreprise.
Règles : ne rien inventer sur mes réglages, me demander de les vérifier. Ne jamais me demander de coller un contenu confidentiel dans cette conversation.
```

Ce que ce guide ne couvre pas

Il ne remplace ni votre contrat de travail, ni la politique de votre entreprise, ni l'avis d'un juriste. Il ne dit rien des autres outils (ChatGPT, Gemini, Copilot), dont les réglages diffèrent. Il s'appuie sur les pages publiques d'Anthropic, de la CNIL et de Google au 1er novembre 2026 : ces pages évoluent.

Savoir quels usages de l'IA sont sûrs dans votre entreprise, lesquels rapportent, et lesquels déconseiller, c'est la matière de notre audit IA : cartographier les tâches poste par poste, puis chiffrer où l'IA vaut le coup.

Pour aller plus loin : Paramétrer Claude : les 6 réglages à faire avant de l'utiliser et Guide décideur : l'IA souveraine en entreprise.

Source. Réglages, conservation et incognito : How long do you store my data, Comment modifier mes paramètres de confidentialité, Use incognito chat, Updates to our consumer terms (28 août 2025), Qui peut voir mes conversations. Plans professionnels : Pricing, Commercial Terms of Service. Connecteurs : Pre-built connectors for Claude, MCP directory policy, Applications tierces d'un compte Google. Samsung : IT-Connect, 7 avril 2023, TechCrunch, 2 mai 2023. Anonymisation : CNIL, 19 mai 2020.
