Partenaires
Action Sociale

LA SÉCURITÉ INFORMATIQUE: LES RÈGLES D'OR

"Un utilisateur averti, c'est un système sécurisé."

Des données sensibles à protéger

Les données manipulées dans PPAS sont confidentielles et concernent un public particulièrement fragile. Leur protection est essentielle pour garantir la fiabilité et la sécurité de l'information.

La sécurité, c'est l'affaire de tous

Chaque utilisateur a un rôle à jouer. En restant vigilant au quotidien, vous contribuez à préserver l'intégrité du système.

Des réflexes simples, des effets durables

Quelques bonnes pratiques suffisent à éviter les erreurs critiques. Ce guide vous aidera à adopter les bons réflexes.

Partenaires
Action Sociale

UN BON MOT DE PASSE, C'EST MA PREMIÈRE LIGNE DE DÉFENSE #1

Mes bonnes pratiques

- Pour créer un mot de passe robuste:
  - **Longueur** : 14 caractères minimum
  - **Complexité** : inclure au minimum une majuscule, une minuscule, un chiffre (conformément aux attentes PPAS), ainsi qu'un ou deux caractères spéciaux (recommandation CNIL)

- Les règles à respecter:
  - Ne jamais utiliser d'informations personnelles (date de naissance, prénom, identifiant, etc.)

"Un bon mot de passe protège vos données et celles des autres."

Partenaires
Action Sociale

MES RÉFLEXES DE SÉCURITÉ #2

"Des gestes simples, une sécurité renforcée."

Mot de passe

- Mon mot de passe est strictement personnel : je ne le partage avec personne, pas même avec mes collègues.
- Je ne laisse jamais mes identifiants visibles sur mon bureau et je ne les enregistre jamais dans le navigateur.
- Je mets à jour mon mot de passe dès que PPAS m'en fait la demande.
- En cas de doute sur une éventuelle divulgation de mon mot de passe, je le change immédiatement.
- J'utilise un mot de passe différent pour chacun de mes comptes personnels.

Poste de travail

- Je verrouille ma session à chaque absence, même brève (Ctrl + Alt + Suppr).
- Avant de quitter mon poste, je me déconnecte systématiquement.

Partenaires
Action Sociale

GESTION DES COMPTES UTILISATEURS POUR L'ADMINISTRATEUR PARTENAIRE#3

- Chaque compte est associé à **une adresse e-mail unique et nominative** ; les adresses e-mail génériques sont à éviter.
- Quand un utilisateur quitte l'organisation, je **supprime** immédiatement son compte et je **ne réutilise pas** ses identifiants.
- Je crée des comptes pour **les nouveaux utilisateurs** dès leur arrivée.
- Si besoin, **plusieurs administrateurs** peuvent être désignés dans une même structure. Cela facilite la gestion sans compromettre la sécurité.

“Une gestion claire des comptes, c’est plus de sécurité et moins d’erreurs”

Partenaires
Action Sociale

PROTECTION DES DONNÉES PERSONNELLES ET SENSIBLES DES BÉNÉFICIAIRES #4

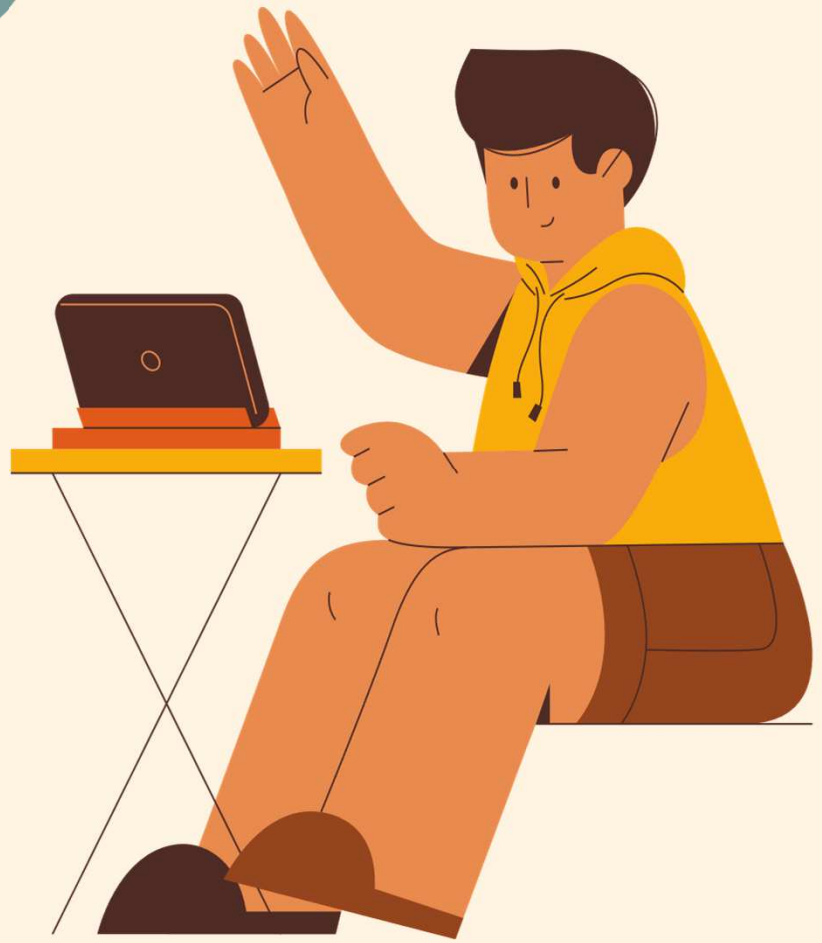
“La collecte et le stockage des données personnelles et sensibles sont soumis à des règles strictes et nécessitent le consentement éclairé de la personne concernée.”

- **Je ne transfère jamais** d’informations professionnelles vers mon espace personnel.
- Je traite toutes les données exclusivement dans **les systèmes sécurisés de l’organisation**.
- Je veille à ce que les données des bénéficiaires ne soient **jamais divulguées à des personnes non autorisées**.
- **Je m’abstiens** de diffuser des données personnelles ou sensibles sur des outils collaboratifs non sécurisés.
- J’utilise des canaux sécurisés pour toute communication de **données personnelles, sensibles ou confidentielles**.

Partenaires
Action Sociale

EN CAS DE SUSPICION DE PIRATAGE OU DE PIRATAGE AVÉRÉ ? #5

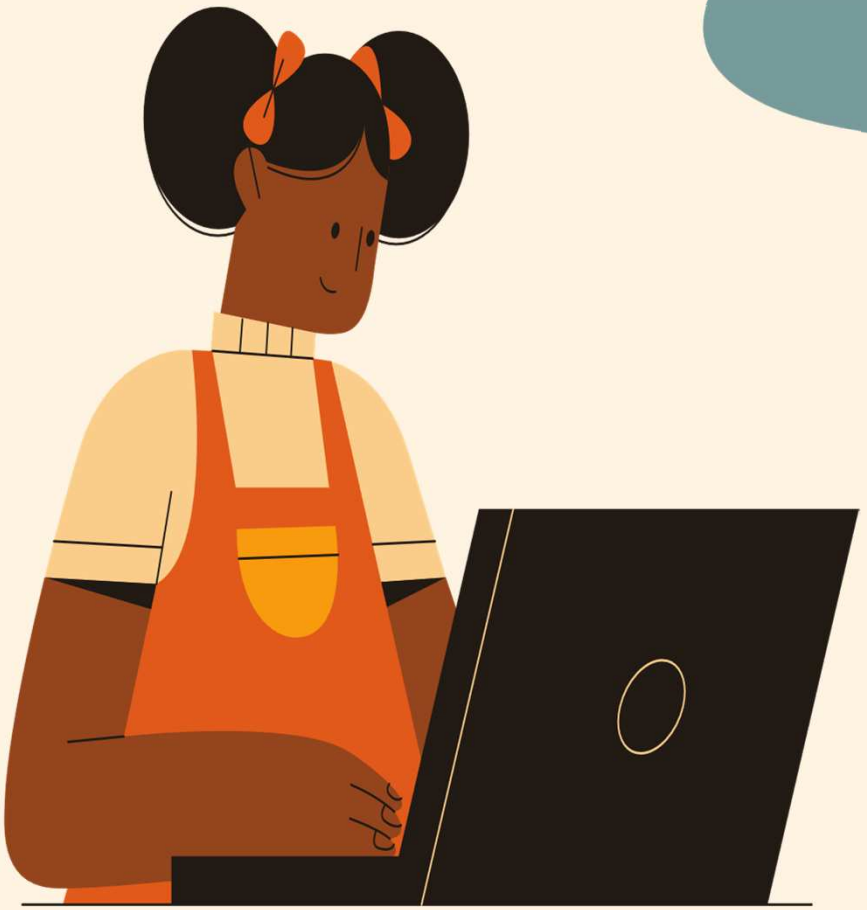
- Je déconnecte immédiatement mon poste d'Internet.
- Je préviens mon responsable hiérarchique et le service informatique.
- Je signale la situation à ma caisse de rattachement.
- Je contacte l'assistance du portail à l'adresse : **webmestre.dijon@carsat-bfc.fr**.



“Plus vite je signale, plus vite je protège mes données .”

Partenaires
Action Sociale

JE RESTE VIGILANT, INFORMÉ ET SOLIDAIRE #6



“La sécurité des systèmes d'information est l’affaire de tous. Chacun a la responsabilité, à son niveau, de garantir la sécurité et la confidentialité des données de l'organisation.”

Mes engagements au quotidien

- Je m'engage à appliquer les consignes de sécurité qui me sont communiquées.
- En cas de problème ou de doute, je réagis immédiatement en suivant les procédures établies.
- Je suis conscient(e) que le non-respect des Conditions Générales d’Utilisation (CGU) peut engager ma responsabilité ainsi que celle de l’organisation.