Parents-thèse	**POLITIQUE NUMERIQUE ET PROTECTION DES DONNEES**	Version : v2.0
	REF: 20260529- OPE-12-04 -Politique numérique et protection des données	Date d'application 2 oct 2026
	Établi par : Claire KORNMANN	
	Validé par : Michel PESCE	8 pages

1. Préambule

L'Association Parents-Thèse inscrit le développement de ses usages numériques dans une démarche continue d'amélioration de la qualité, de sécurisation des accompagnements et de respect des droits des personnes accompagnées, de leurs représentants légaux et des professionnels.
Les outils et services numériques contribuent à la coordination des interventions, à la traçabilité des accompagnements, au partage des informations, à la continuité des activités et au fonctionnement de l'Association.
Leur utilisation implique toutefois une vigilance particulière concernant :

- la protection des données à caractère personnel ;
- le respect de la vie privée et de la confidentialité ;
- la sécurité des systèmes d'information et des équipements ;
- la maîtrise des accès et des habilitations ;
- la continuité des activités ;
- les usages numériques en mobilité et hors des locaux ;
- la prévention et la gestion des incidents numériques ;
- l'usage responsable, éthique et sécurisé des outils numériques et de l'intelligence artificielle.

La présente politique définit les **orientations et principes directeurs de l'Association Parents-Thèse en matière de numérique, de sécurité de l'information et de protection des données**.
Elle s'inscrit dans le cadre défini par le règlement intérieur et est déclinée, selon les domaines concernés, par les chartes, procédures, protocoles, consignes et fiches réflexes applicables au sein de l'Association.

2. Finalités de la Politique numérique

L'association Parents-Thèse poursuit les objectifs suivants :

2.1. Garantir les droits des personnes

L'Association veille à ce que les usages numériques respectent les droits des personnes accompagnées, de leurs représentants légaux et des professionnels.

Elle s'engage notamment à :

- respecter la vie privée et la confidentialité ;
- protéger les données à caractère personnel qui lui sont confiées ;
- garantir un accès aux informations adapté aux missions et responsabilités de chacun ;
- permettre l'exercice des droits reconnus aux personnes par la réglementation applicable ;
- veiller à ce que le développement des usages numériques demeure compatible avec le respect des droits fondamentaux des personnes.

2.2. Soutenir la qualité et la continuité des activités

Les outils numériques contribuent à :

- améliorer la coordination entre les professionnels ;
- assurer une traçabilité sécurisée des accompagnements et des activités ;
- faciliter la communication avec les personnes accompagnées, les familles et les partenaires ;
- soutenir la continuité des interventions et des activités ;
- permettre un partage d'informations pertinent, proportionné et sécurisé ;
- faciliter l'accès des professionnels aux informations et ressources nécessaires à l'exercice de leurs missions.

2.3. Prévenir les risques numériques

L'Association veille à prévenir les risques susceptibles d'affecter la sécurité de ses systèmes d'information, la confidentialité, l'intégrité et la disponibilité des données ainsi que la continuité de ses activités.
Elle s'attache notamment à :

- prévenir les accès non autorisés, pertes, altérations ou divulgations de données ;
- sécuriser les équipements, applications, comptes et accès numériques ;
- prévenir les risques liés aux erreurs humaines, aux usages inadaptés et aux cyberattaques ;
- maîtriser les risques liés aux usages numériques en mobilité et hors des locaux ;
- organiser la détection, le signalement et le traitement des incidents numériques et des violations de données ;
- assurer, lorsque cela est nécessaire, la continuité et la restauration des activités et des données.

A VALIDER

2.4. Accompagner l'évolution des pratiques

L'Association veille à développer :

- les compétences numériques des professionnels ;
- une culture commune de protection des données et de cybersécurité ;
- l'appropriation des outils numériques institutionnels ;
- des usages numériques responsables et proportionnés ;
- un usage raisonné, éthique et sécurisé de l'intelligence artificielle ;
- une culture de vigilance et de signalement des incidents.

3. Principes directeurs

3.1. Principe de confidentialité

Les informations relatives aux personnes accompagnées, à leurs familles, aux professionnels et au fonctionnement de l'Association sont protégées conformément à leur nature et au cadre juridique applicable.

L'accès aux informations est limité aux personnes autorisées qui en ont besoin dans le cadre de leurs missions.

Le partage d'une information s'effectue dans le respect des règles de confidentialité, de secret professionnel et de partage d'informations applicables.

3.2. Principe de proportionnalité

Les données et informations sont collectées, consultées, utilisées, transmises et conservées dans la mesure nécessaire aux finalités poursuivies et à l'accomplissement des missions de l'Association.

3.3. Principe de sécurité

L'Association met en œuvre des mesures techniques et organisationnelles adaptées visant à garantir :

- la confidentialité des données ;
- leur intégrité ;
- leur disponibilité ;
- leur traçabilité ;

AVALIDER

- la maîtrise des accès aux systèmes et aux informations.

3.4. Principe d'habilitation et de maîtrise des accès

L'accès aux applications, espaces numériques, dossiers et informations est attribué en fonction des missions exercées et du besoin d'en connaître.

L'Association organise la création, l'attribution, l'évolution et la suppression des habilitations afin de maintenir des droits d'accès adaptés à la situation professionnelle de chaque utilisateur.

Les accès sont personnels et leur utilisation engage la responsabilité de leur titulaire.

3.5. Principe de responsabilité partagée

La sécurité numérique et la protection des données reposent sur une responsabilité partagée entre l'Association et les différents acteurs intervenant, selon leurs fonctions et responsabilités, dans la gestion des données, des systèmes d'information et des outils numériques.

Chaque professionnel contribue, dans le cadre de ses fonctions, à la protection des informations et des outils qui lui sont confiés et participe à la prévention et au signalement des incidents.

Les responsabilités des différents acteurs sont précisées dans les procédures et documents institutionnels applicables.

3.6. Principe de continuité

L'Association organise la continuité de ses activités afin de limiter les conséquences d'une indisponibilité des systèmes d'information, d'un dysfonctionnement informatique ou d'un cyberincident.

4. Finalités du traitement des données

L'Association met en œuvre des traitements de données à caractère personnel nécessaires à l'exercice de ses missions, à l'accompagnement des personnes, à son fonctionnement administratif et à la gestion de ses activités.

A VALIDER

Ces traitements sont mis en œuvre pour des finalités déterminées, explicites et légitimes et dans le respect des principes applicables à la protection des données.

L'Association veille notamment à la pertinence des données traitées, à la maîtrise de leur accès, à leur durée de conservation et à l'information des personnes concernées.

Les traitements mis en œuvre et leurs caractéristiques sont documentés dans les outils de conformité prévus à cet effet.

5. Gouvernance de la protection des données

La Direction définit, valide et pilote la politique numérique et de protection des données de l'Association.
Sa mise en œuvre repose sur une responsabilité partagée et mobilise, selon leurs fonctions et domaines de compétence :

- la Direction ;
- les responsables hiérarchiques ;
- le Délégué à la protection des données (DPO) ;
- la fonction qualité / QSE-RSE ;
- les administrateurs et prestataires des systèmes d'information ;
- les professionnels utilisateurs des outils numériques.

Le DPO informe et conseille l'Association sur ses obligations en matière de protection des données personnelles. Il contribue au suivi de la conformité, conseille l'Association sur les questions relatives à la protection des données et constitue le point de contact avec l'autorité de contrôle. Il peut être consulté par les professionnels et les personnes concernées dans son champ de compétence.

La fonction Qualité / QSE-RSE contribue, en lien avec la Direction et le DPO, à l'intégration de la protection des données dans la démarche qualité et de gestion des risques, au suivi du dispositif documentaire ainsi qu'aux actions de sensibilisation et d'amélioration continue.
Les responsabilités opérationnelles et les circuits de traitement sont précisés dans les procédures et documents applicables.
Le pilotage de la politique numérique s'inscrit dans la démarche d'amélioration continue et de gestion des risques de l'Association.

6. Engagements de l'Association

VALIDER

6.1. Protection des données et des droits

L'Association s'engage à :

- respecter la réglementation applicable en matière de protection des données ;
- assurer la confidentialité des informations qui lui sont confiées ;
- informer les personnes concernées sur l'utilisation de leurs données et leurs droits ;
- organiser l'exercice de ces droits ;
- intégrer la protection des données dans l'évolution de ses pratiques et de ses outils.

6.2. Sécurité numérique

L'Association s'engage à :

- sécuriser les équipements, applications et accès ;
- organiser la gestion des habilitations ;
- maintenir les systèmes dans des conditions de sécurité adaptées ;
- mettre en œuvre des mesures de sauvegarde et de continuité appropriées ;
- prévenir les risques de cyberattaque, de fraude et de compromission des données.

6.3. Prévention et gestion des incidents

L'Association favorise une culture de vigilance et de signalement des incidents et anomalies numériques.

Tout incident ou suspicion d'incident susceptible d'affecter la confidentialité, l'intégrité, la disponibilité ou la sécurité des données et des systèmes fait l'objet d'un signalement et d'une prise en compte selon les procédures applicables.

L'Association organise l'analyse des événements et incidents et la mise en œuvre des mesures nécessaires. Le DPO est associé à l'analyse lorsque l'incident concerne ou est susceptible de concerner des données à caractère personnel.

Les événements significatifs donnent lieu, lorsque cela est pertinent, à des actions correctives, préventives et à un retour d'expérience.

6.4. Accompagnement des professionnels

L'Association veille à :

- informer et sensibiliser régulièrement les professionnels ;
- accompagner leur prise en main des outils institutionnels ;

A VALIDER

- développer leurs compétences numériques ;
- diffuser les procédures, consignes et fiches réflexes nécessaires ;
- favoriser le retour d'expérience et le partage des bonnes pratiques.

7. Usage responsable de l'intelligence artificielle

L'Association reconnaît l'intérêt potentiel des systèmes et outils d'intelligence artificielle pour soutenir certaines activités professionnelles.
Leur utilisation s'inscrit dans une démarche responsable, proportionnée, transparente et sécurisée.

L'intelligence artificielle constitue un outil d'assistance et ne se substitue ni au jugement professionnel, ni à la décision humaine, ni aux responsabilités attachées aux fonctions exercées.

Une vigilance particulière est portée à la confidentialité des informations, à la protection des données, à la fiabilité des résultats produits et à la maîtrise des outils utilisés.

Les données permettant d'identifier directement ou indirectement une personne accompagnée, un membre de sa famille ou un professionnel ne sont pas introduites dans un outil d'intelligence artificielle qui n'a pas été expressément autorisé à cet effet par l'Association.

Les conditions et règles d'utilisation des outils d'intelligence artificielle sont précisées dans les documents institutionnels applicables.

8. Documents de référence et documents associés

La présente politique s'articule notamment avec :
Document de référence :

- Règlement intérieur de l'Association Parents-Thèse.

Documents de déclinaison :

- Charte des usages numériques ;
- procédure relative à la protection des données personnelles ;
- procédures relatives à la structuration, à la tenue, à l'accès et à la consultation du DUI ;
- procédure relative au partage d'informations à caractère secret ;
- procédure relative à la gestion des violations de données ;

AVALIDER

- procédure relative à l'archivage et à la destruction des documents ;
- dispositions relatives aux habilitations et aux accès numériques ;
- dispositions relatives au travail hors des locaux et aux usages numériques en mobilité ;
- Plan de continuité d'activité ;
- procédure de gestion des événements indésirables ;
- fiches réflexes relatives à la cybersécurité et à la protection des données.

Cette liste est susceptible d'évoluer en fonction des besoins, des outils utilisés et du système documentaire de l'Association.

9. Évaluation et amélioration continue

La présente politique fait l'objet d'une évaluation régulière dans le cadre de la démarche d'amélioration continue de l'Association Parents-Thèse. Son évaluation s'appuie notamment sur :

- les incidents et événements déclarés ;
- les retours d'expérience des professionnels ;
- les résultats des évaluations, audits et contrôles ;
- l'évolution des risques numériques ;
- l'évolution des pratiques et des systèmes d'information ;
- les évolutions réglementaires et technologiques.

La politique est réexaminée périodiquement et chaque fois qu'une évolution significative du contexte réglementaire, organisationnel, technologique ou du système d'information le justifie.

AVALIDER