Politique interne de protection des données du COLLEGE NOTRE-DAME

1. **Pourquoi une politique interne de protection des données ?** Notre institution collecte et traite de nombreuses informations à caractère personnel relatives aux personnes physiques : élèves/étudiants, parents, membres du personnel, fournisseurs, partenaires et toute personne avec qui notre établissement entretient des relations.

   La présente politique interne de protection des données décrit comment ces données à caractère personnel doivent être collectées, traitées et stockées pour rencontrer les standards de protection et maintenir celle-ci en conformité avec la loi et le règlement général de protection des données (RGPD).

   Notre institution est responsable de sa conformité aux lois relatives à la protection des données personnelles et doit être capable de démontrer celle-ci à tout moment, notamment auprès de l'autorité de contrôle. Pour la Belgique, la loi du 3 décembre 2017 a transformé la Commission vie privée en une Autorité de protection des données (« APD ») et lui a conféré les pouvoirs nécessaires pour (entre autres) pouvoir appliquer les nouvelles sanctions en cas de violation des dispositions du RGPD.

2. **A qui et à quoi s'applique cette politique de protection des données ?** Cette politique s'applique à toutes les opérations que notre institution réalise sur des données à caractère personnel. Ce code de conduite doit donc être respecté par tous les membres du personnel, quel que soit leur fonction et leur statut, en ce compris la Direction, les volontaires, les stagiaires et les membres du Pouvoir organisateur.

   Les traitements de données à caractère personnel sont toute action (collecte, encodage, reproduction, transformation, partage, effacement...) exercée sur des données relatives à des personnes physiques identifiées ou identifiables (entre autres le personnel de l'institution scolaire ou du CPMS, d'employés, de fournisseurs, de personnes de contact auprès d'autres institutions, d'élèves, de parents, des membres du Pouvoir organisateur, etc).

   La Politique de protection des données à caractère personnel est adoptée et peut être mise à jour par la direction de l'institution.

   Le P.O. a désigné un « Délégué à la protection des données » (voir point 7) qui conseille le P.O. et la direction au sujet de la protection des données à caractère personnel, contrôle la bonne mise en œuvre du RGPD, informe les MDP et les élèves / étudiants et est le point de contact pour l'exercice de leurs droits.

3. **Quel est le droit applicable ?** Diverses lois et régulations nationales et internationales protègent les droits des individus en ce qui concerne leur vie privée et le traitement des données les concernant, en ce compris le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données : ci-après "RGPD"). Certains termes utilisés dans cette Politique ont des significations particulières, ces significations étant établies à l'article 4 du RGPD.

4. **Principes généraux.** Les données à caractère personnel traitées par ou au nom du P.O. et de notre institution doivent être faits conformément aux principes généraux ci-dessous.

   Toutes les données personnelles doivent être traitées de manière **légale, loyale** et **transparente**. Ainsi les données ne peuvent être traitées que si une des conditions suivantes est satisfaite :

   - La personne concernée a donné son consentement ;
   - Le traitement est nécessaire pour l'exécution du contrat auquel la personne concernée est partie ou, à la demande de la personne concernée, dans les étapes précédant la conclusion d'un contrat dans l'optique de conclure ce contrat ;
   - Le traitement est nécessaire pour que le P.O. et notre institution scolaire soient en conformité avec ses obligations légales ;
   - Le traitement est nécessaire en vue de protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ;
   - Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont serait investi le P.O. ;
   - Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le P.O ;

   Les données à caractère personnel ne peuvent être traitées qu'à des fins clairement limitées et définies qui sont licites et qui ont été communiquées à la personne concernée avant que le traitement n'ait eu lieu. Elles ne peuvent pas être traitées à une autre fin.

   Le P.O. et notre institution ont une obligation de minimisation des données : elles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

   Toutes les données à caractère personnel doivent être précises, complètes et tenues à jour. Dans la mesure du possible, toute donnée inexacte, incomplète ou périmée doit être corrigée ou effacée.

   Les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire. A défaut d'une obligation légale de conservation imposée à notre établissement, elles doivent être supprimées lorsqu'elles ne sont plus utiles.

   Il est interdit de transférer ou divulguer des données à caractère personnel sans que la personne concernée ait consenti au transfert ou que ce transfert ne soit nécessaire pour l'exécution d'un contrat, auquel la personne concernée est partie, ou, à la demande de la personne concernée dans les étapes précédant la conclusion d'un contrat, dans l'optique de conclure ce contrat, ou à moins que ce transfert ne soit imposé par la loi ou un cadre règlementaire.

   Toutes les données à caractère personnel traitées par ou au nom du P.O. et notre institution doivent faire l'objet de mesures organisationnelles et de sécurité appropriées pour s'assurer

Sécurité informatique :

- Ne partagez jamais vos mots de passe.
- Verrouillez votre session informatique lorsque vous quittez votre poste.
- Ne dupliquez pas les fichiers contenant des données personnelles et nettoyez régulièrement votre dossier de téléchargement.

Gestion des documents papier : Ne laissez pas de documents contenant des données personnelles à la vue de tous. Les documents papier obsolètes doivent être broyés ou jetés dans la corbeille sécurisée.

5. Que faire en cas d'incident ou de fuite de données ?

Une fuite de données peut résulter d'un vol/perte de matériel (PC, clé USB, smartphone), d'un courriel envoyé au mauvais destinataire, d'un piratage ou d'un virus.

Procédure d'urgence : Si vous suspectez ou constatez la perte, le vol ou l'accès non autorisé à des données personnelles, vous devez en informer immédiatement et sans délai la Direction et le DPO afin de permettre la prise de mesures correctives.

6. Sanctions

Le non-respect délibéré ou répétitif des consignes de protection des données constitue une faute susceptible de donner lieu à des mesures ou sanctions disciplinaires, conformément au Règlement de travail et aux statuts applicables.

Document adopté le 1er décembre 2025

Pour le Pouvoir Organisateur / La Direction

