Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche
Académie d'Orléans-Tours

Lycée polyvalent François Rabelais
28, quai Danton
37 500 CHINON
FRANCE

REGLEMENT INTERIEUR SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Acte du Conseil d'administration n°

Vu le Code de l'éducation ;

Vu le Code des relations entre le public et l'administration ;

Vu la Loi n° 78-17 du 06 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la Loi n° 2004-801 du 06 Août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu le règlement européen UE 2016/679 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 ;

Vu la Loi n° 2016-1321 du 07 Octobre 2016 pour une République numérique dite Loi Lemaire ;

Vu la Loi n° 2018-493 du 20 Juin 2018 relative à la protection des données personnelles ;

Vu le décret n° 2018-687 du 01 Août 2018 pris pour l'application de la Loi n° 78-17 du 06 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n° 2018-493 du 20 Juin 2018 relative à la protection des données personnelles

Vu le décret n° 2019-341 du 19 Avril 2019 relatif à la mise en oeuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire.

PREAMBULE :

Le présent règlement intérieur vise à consigner l'ensemble des principes, règles et procédures afférentes au traitement, à la gestion et à la protection des données à caractère personnel des usagers du service public manipulées par les personnels du lycée polyvalent François Rabelais.

Il vise notamment à garantir à ces derniers, les principes suivants :

- égalité de traitement dans les procédures d'examen et d'instruction administrative, budgétaire, comptable et financière, par la garantie déontologique, éthique et légale, d'application d'un cadre normatif préalablement défini ;
- transparence dans le respect des informations personnelles et nominatives transmises aux différents services du lycée polyvalent François Rabelais et à l'ensemble de ses partenaires ;

- constance et régularité des procédures applicables, dans la limite des modifications normatives imposées.

Le présent document dénommé « règlement intérieur sur la protection des données à caractère personnel » vaut règlement général sur la protection des données à caractère personnel dans sa déclinaison locale spécifiquement applicable au lycée polyvalent François Rabelais.

Le lycée polyvalent François Rabelais, possède la personnalité morale. Etablissement public local d'enseignement, il est libre de conclure tout contrat ou convention nécessaire à ses activités.

TITRE 1 : CADRE REGLEMENTAIRE

Article 1 : DEFINITIONS ET CHAMPS D'APPLICATION TERMINOLOGIQUES :

Article 1.1 : La notion de donnée à caractère personnel :

Est considérée donnée à caractère personnel, toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.

Ainsi peut-il s'agir d'un nom, d'une photo, d'une empreinte, d'une adresse postale, d'une adresse courriel, d'un numéro de téléphone, d'un numéro d'inscription sur un registre officiel, d'un matricule interne, d'une adresse I.P, d'un identifiant de connexion informatique, d'un enregistrement vocal ou de tout autre instrument renvoyant à l'identité numérique d'une personne physique.

Le caractère confidentiel ou public de ces informations ne peut être retenu. L'anonymisation des données retranche à ces dernières leur caractère personnel. A contrario, s'il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme…) ou par l'utilisation de moyens techniques divers, d'identifier une personne physique, les données concernées sont toujours considérées comme personnelles.

Article 1.2 : La notion de donnée sensible :

Les données sensibles sont constituées d'informations révélant la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ainsi que le traitement des données génétiques ou biométriques aux fins d'identification d'une personne physique de manière unique, de données relatives à la santé ou concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

L'utilisation et la collecte de ces données sont strictement interdites au sein de l'établissement à l'exception des cas dérogatoires suivants, prévus par la réglementation applicable :

- si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique et informée) ;
- si les informations sont manifestement rendues publiques par la personne concernée ;
- si elles sont nécessaires à la sauvegarde de la vie humaine ;
- si leur utilisation est justifiée par l'intérêt public et autorisé par la Commission nationale informatique et liberté ;
- si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

Article 1.3 : Identité personnelle, identité numérique et e-réputation :

L'identité personnelle se définit comme l'ensemble des informations qui rendent une personne singulière et unique.

L'identité numérique est constituée de l'ensemble des traces numériques qu'une personne ou une collectivité laisse sur Internet ou tout support dématérialisé.

L'identité numérique peut être constituée des mêmes éléments caractérisant une donnée à caractère personnel. En cela, l'identité numérique est indissociable de l'e-réputation. Celle-ci se définit comme la perception qu'une personne physique souhaite donner d'elle sur Internet ou tout support dématérialisé.

Article 2 : LE RESPONSABLE DE TRAITEMENT :

Le responsable d'un traitement de données à caractère personnel peut être une personne physique, une autorité publique ou un organisme déterminant les finalités et moyens de traitement, de gestion et de conservation d'un fichier informatique et qui en décide la création.

Le lycée polyvalent François Rabelais, à travers son Chef d'établissement, est désigné par le présent document, responsable du traitement des fichiers dématérialisés exploités au sein de l'établissement à l'exception des fichiers manipulés par les services mutualisateurs installés au sein de celui-ci, pour lesquels la convention constitutive peut décider d'y déroger.

Le responsable du traitement doit accomplir lorsque cela est obligatoire les formalités déclaratives auprès de la Commission nationale informatique et libertés. Il est tenu de démontrer que le traitement des données à caractère personnel réalisé sous sa responsabilité est conforme à la réglementation en la matière. Cette responsabilité ne peut être transférée au Délégué à la protection des données par délégation de pouvoir sans constituer effectivement un conflit d'intérêts.

Article 2.1 : Le représentant du responsable de traitement :

Est désigné représentant du responsable de traitement, l'Adjoint au Chef d'établissement en charge des affaires pédagogiques et éducatives.

Le représentant est mandaté par le responsable du traitement pour être l'interlocuteur privilégié des autorités de contrôle en lieu et place du responsable du traitement, pour toutes les questions relatives au traitement, aux fins d'assurer le respect du présent règlement.

La désignation d'un représentant par le responsable du traitement est sans préjudice d'actions en justice qui pourraient être intentées contre le responsable du traitement lui-même.

Article 3 : LE DELEGUE A LA PROTECTION DES DONNEES :

Article 3.1 : Compétences, prérequis techniques et incompatibilités fonctionnelles :

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et en particulier ses connaissances spécialisées du droit et des pratiques en matières de protection des données et de sa capacité à accomplir les missions qui lui sont dévolues. A ce titre, il doit démontrer :

- une aptitude à communiquer efficacement et à exercer ses fonctions et missions en toute indépendance ;
- l'absence de toute implication dans d'éventuels conflits d'intérêts avec ses autres missions. Il ne peut donc occuper de fonctions, au sein de l'établissement, le conduisant à déterminer les finalités et les moyens d'un traitement.
- une expertise en matière règlementaire et pratique spécifique à la protection des données. Le niveau d'expertise doit être adapté à l'activité de l'établissement et à la sensibilité des traitements mis en œuvre ;
- une bonne connaissance du secteur d'activité et de l'organisation interne de l''établissement en particulier des opérations de traitement, des systèmes d'information et des besoins de l'établissement en matière de protection et de sécurité des données :
- un positionnement interne de nature à lui permettre de faire directement rapport au niveau de responsabilité le plus élevé, d'animer un réseau.

Les missions propres au Délégué à la protection des données sont incompatibles avec celles de responsable de traitement, d'administrateur réseau, d'opérateur réseau (fournisseur d'accès internet, technicien de l'information et de la communication…).

Dans l'éventualité où le Délégué à la protection des données dirige un service mutualisateur, ce dernier ne peut être désigné responsable de traitement dudit service.

Cette fonction est alors automatiquement transférée au personnel de ce service le plus gradé, indépendamment des dispositions éventuellement contradictoires de la convention mutualisatrice concernée.

Article 3.2 : Rôle et missions :

Le Délégué à la protection des données est principalement chargé :

- d'informer et de conseiller le responsable de traitement ou son représentant ainsi que les personnels en responsabilité quant aux risques associés aux opérations de traitement et aux évolutions règlementaires intervenant en la matière ;
- d'établir une politique de protection des données à caractère personnel et mettre en œuvre des procédures transversales (notification au responsable de traitement des violations constatées, mise en oeuvre des mentions légales et règlementaires obligatoires dans les documents utilisés par l'établissement…) ;
- de promouvoir les bonnes pratiques et les gestes techniques visant à garantir l'identité numérique des usagers et de contribuer à l'éducation numérique de ces derniers ;
- de contrôler le respect de la réglementation en matière de protection des données ;
- de conseiller l'établissement quant à la réalisation éventuelle d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- d'assurer la tenue du registre des traitements mis en œuvre au sein de l'établissement ;
- d'assurer la publicité effective des droits et obligations des usagers du service public en matière de protection des données ;
- d'instruire en premier recours les plaintes des usagers de l'établissement ;
- d'assurer la liaison avec les autorités de contrôle (Délégué académique à la protection des données, Commission nationale informatique et liberté, juridictions nationales et étrangères…).

Le Délégué à la protection des données n'est pas personnellement responsable en cas d'infraction ou de non-conformité de l'établissement avec la réglementation applicable à la protection des données à caractère personnel.

Article 3.3 : Obligations statutaires et protection réglementaire :

Le Délégué à la protection des données doit agir en toute indépendance et bénéficier dans l'exercice de ses missions d'une protection suffisante et effective du responsable du traitement ou de son représentant.

Il est soumis à une stricte obligation de confidentialité, de discrétion et de secret professionnels. Cependant, il n'est pas astreint au devoir de réserve envers le Responsable du traitement dans l'instruction des plaintes déposées à son encontre par les usagers et dans la communication et les échanges qu'il entretient avec les autorités de contrôle.

Afin d'assurer une continuité et une permanence effective des missions confiées, seul un personnel titulaire d'un concours de la Fonction publique d'Etat peut être désigné Délégué à la protection des données.

Il est à noter que le Délégué à la protection des données ne peut en aucun cas, être sanctionné du fait de l'exercice des missions qui lui sont dévolues.

Article 3.4 : Moyens d'actions :

Le Délégué à la protection des données doit bénéficier du soutien de l'établissement qui le désigne. Ainsi, sa désignation doit être approuvée par un vote du Conseil d'administration dudit établissement.

Ce dernier doit :

- s'assurer de son implication dans toutes les questions relatives à la protection des données en le conviant à toute réunion de travail impactant son domaine de compétence ;
- lui fournir les ressources nécessaires à la réalisation de ses missions en le conviant à des formations, en lui en octroyant le temps nécessaire ou en lui attribuant les ressources matérielles ou financières adéquates ;
- lui faciliter l'accès aux données et opérations de traitement par un accès facilité aux autres services de l'établissement et à la consultation par ses soins des fichiers mis en œuvre.
- veiller à l'absence de conflit d'intérêts.

TITRE 2 : DES DROITS ET OBLIGATIONS DES INTERVENANTS

Article 4 : DES DROITS DES USAGERS DU SERVICE PUBLIC D'EDUCATION :

Les usagers du service public peuvent :

- être informés sur l'utilisation et le traitement des données personnelles qui les concernent, sur leurs droits inhérents et les voies de recours éventuels ;
- s'opposer à tout moment à l'utilisation de leurs données personnelles. Ce droit est cependant inopposable lorsque ces données sont indispensables à l'exercice d'une mission d'intérêt général.
- obtenir et vérifier leurs données personnelles auprès du responsable du traitement habilité ;
- demander au responsable du traitement la rectification ou l'effacement de toute donnée personnelle les concernant ;
- formuler plainte auprès du Délégué à la protection des données de l'établissement et de toute autre autorité de contrôle ;
- obtenir du Délégué à la protection des données ou de toute autre autorité de contrôle, le rétablissement des droits dont il s'estime lésé.

Les usagers du service public d'éducation ont également le droit au respect de leur image et de leur voix.

D'autres droits sont également consacrés par la réglementation mais sont inopposables au lycée polyvalent François Rabelais dans l'exercice de ses activités de service public.

Article 5 : LES OBLIGATIONS DU RESPONSABLE DE TRAITEMENT :

Le responsable de traitement a obligation d'assurer une information complète, sincère et loyale des usagers du service public d'éducation.

De fait, l'ensemble des courriers, formulaires ou documents intégrant des données à caractère personnel doit intégrer les mentions légales et réglementaires.

En outre, le responsable de traitement met à disposition de ses usagers, les formulaires dédiés et spécifiques au respect de leur image ou de leur voix, notamment pour ce qui a trait aux personnes physiques mineures.

La communication des droits et obligations de chaque intervenant en matière de protection des données à caractère personnel peut intervenir via affichage, via le site internet de l'établissement ou par tout

autre moyen jugé adéquat et dont le responsable de traitement pourra apporter la preuve en cas de contestation ou plainte.
Le responsable du traitement a obligation de collaborer avec les autorités de contrôle, à la demande de celles-ci, dans l'exécution de ses missions.

Article 5.1 : Utilisation des technologies de l'information et de la communication dans l'enceinte de l'établissement :

Chaque personne physique, qu'elle soit majeure ou mineure, est personnellement responsable des données qu'elle consulte ou diffuse via une technologie de l'information et de la communication dont elle est propriétaire (téléphone portable, tablette, dispositif de géo-localisation, objets connectés de toute nature…). Il en résulte qu'une plainte d'un usager fondée sur l'utilisation d'appareils lui appartenant ou appartenant à un tiers serait de fait, déclarée irrecevable par le Délégué à la protection des données.

A l'inverse, les obligations pesant sur le responsable de traitement ont vocation à s'appliquer dès lors qu'une technologie de l'information ou de la communication lui appartenant ou dont il a reçu dotation a été mise à disposition d'un de ses usagers.

Article 5.2 : Connexion d'appareils tiers aux réseaux informatiques et de télécommunications internes à l'établissement :

S'agissant de la connexion d'appareils tiers ou appartenant à des usagers de l'établissement, ce dernier endosse, au surplus des obligations pesant sur le responsable de traitement, celles pesant sur un fournisseur d'accès, internet ou téléphonique et encourt les sanctions pénales et administratives qui y sont inhérentes. Le responsable du traitement s'assure de la mise en œuvre de mesures de protection limitatives (interdiction d'accès aux réseaux sociaux ou à tout autre site à contenu pornographique ou intégrant des propos, images ou discours faisant l'apologie du terrorisme, incitant à la haine ou la discrimination, ou à la violation des Lois et règlements de la République…).

Concrètement, le Délégué à la protection des données ne pourra déclarer irrecevable une plainte d'un usager quand bien même celui-ci aurait lui-même contribué au préjudice qu'il aurait subi du fait de la diffusion ou de la communication d'un ou plusieurs éléments de son identité numérique.

Article 6 : REGISTRE DES ACTIVITES DE TRAITEMENT :

Le responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :

- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
- les finalités du traitement ;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, si besoin, les documents attestant de l'existence de garanties appropriées;
- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

Au regard des compétences spécifiques du Délégué à la protection des données, le responsable du traitement peut lui déléguer la tenue de ce registre.

Le responsable du traitement ou le Délégué à la protection des données mettent le registre des activités de traitement à disposition de l'autorité de contrôle qui en fait la demande.

TITRE 3 : PLAINTES ET VIOLATIONS PENALES

Article 8 : VIOLATIONS DE DONNEES A CARACTERE PERSONNEL ET PROCEDURE INTERNE :

La violation de données à caractère personnel est constituée dès lors, qu'en cours de traitement, celles-ci ont fait l'objet d'une perte de disponibilité, d'intégrité ou de confidentialité de manière accidentelle ou illicite.

Une enquête interne est immédiatement diligentée par le Délégué à la protection des données et vise notamment à déterminer :

- la nature et la gravité de la violation constatée ;
- si possible, les catégories et le nombre approximatif de personnes concernées par la violation dont il est question ;
- les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- les conséquences probables de la violation de données ;
- les mesures prises ou envisagées pour éviter que cet incident ne se reproduise ou pour en atténuer les éventuelles conséquences négatives.

Une fiche d'incident est nécessairement annexée au registre des traitements et transmise simultanément à la Commission nationale informatique et liberté ainsi qu'au Délégué académique à la protection des données, idéalement dans un délai maximum de 72 heures suivant la constatation effective de la violation par le Délégué à la protection des données de l'établissement.

La gravité de la violation constatée est évaluée par le Délégué à la protection des données selon l'échelle suivante :

- minimale : violation sans perte de données ou menace sur l'intégrité des équipements informatiques et systèmes de cybersécurité ;
- moyenne : violation avec perte de données mais sans menace sur l'intégrité des équipements informatiques et systèmes de cybersécurité ;
- maximale : violation avec perte de données et menace sur l'intégrité des équipements informatiques et systèmes de cybersécurité.

Les personnes concernées par une violation dont la gravité maximale est avérée se verront notifier l'incident par le responsable du traitement.

Article 8.1 : Cyberattaques, piratages et opérations tiers malveillantes :

Toute tentative d'intrusion malveillante au sein des systèmes informatiques du responsable de traitement fera l'objet d'un dépôt de plainte systématique auprès des services de Police nationale ou Gendarmerie. Le responsable du traitement, associé au Délégué à la protection des données s'engagent à tenir à disposition des enquêteurs tous les éléments de preuves techniques en leur possession, voire, le cas échéant, à en assurer la sauvegarde sur tout support ad'hoc.

Ce dépôt de plainte peut également être assorti d'un signalement sur la plate-forme http://www.cybermalveillance.gouv.fr/

Il en va de même pour les tentatives de piratage quelles que soient leurs formes et les procédés techniques utilisés (attaques Ddos, arnaques à l'hameçonnage, vols ou usurpation d'identité ou de données, kits d'exploits, ransomwares, malwares, spywares, trackers, phishing, pharming, keylogging, sniffing, cryptojacking…) destinées à gêner ou paralyser le fonctionnement de l'établissement.

Toute opération tiers malveillante ayant eu pour effet de compromettre l'intégrité financière de l'établissement sera au surplus des mesures précédemment énoncées, notifiée, par le comptable public assignataire, auprès des partenaires institutionnels spécifiques de l'établissement (Direction générale des Finances publiques, Banque de France, Caisse des dépôts et consignations…).

Article 9 : PROCEDURE DE DEPOT DE PLAINTE APPLICABLE AUX USAGERS :

L'usager s'estimant lésé dispose de la faculté de déposer plainte auprès des autorités chargées du contrôle du respect de ses droits en matière de protection des données à caractère personnel.
Concrètement, le lycée polyvalent François Rabelais met en œuvre un système de dépôt de plainte à trois niveaux :

- premier niveau : le Délégué à la protection des données qui dispose d'un délai de deux mois pour instruire la plainte qui lui est soumise, formuler réponse à l'usager lésé, proposer le cas échéant au responsable de traitement les mesures de remédiation adéquates ou saisir une autorité de contrôle supérieure ;
- deuxième niveau : le Délégué académique à la protection des données collaborant avec le Délégué à la protection des données de l'établissement ;
- troisième niveau : la Commission informatique et liberté instruisant la plainte indépendamment des autorités de contrôle sus-citées mais pouvant auditionner ces dernières en cas de besoin.

Aucune réclamation ou plainte ne sera instruite si elle n'est pas préalablement formalisée par écrit.

Afin d'obtenir une réponse rapide et efficace, il est recommandé à l'usager s'estimant lésé de saisir les autorités de contrôle mentionnées au présent article dans l'ordre d'instruction décrit : premier niveau puis deuxième niveau et enfin troisième niveau.