FNEC FP
FO

Montreuil, le 23 août 2026
M. Edouard Geffray
Ministre de l'Education nationale
110, rue de Grenelle 75007 PARIS

Objet : Cyberattaques et fuites de données à l'Education nationale

Monsieur le Ministre,

La rentrée scolaire s'annonçait déjà chaotique avec les milliers de suppressions de postes et de classes et la dégradation continue des conditions de travail liée aux contre-réformes… les systèmes informatiques du ministère viennent à nouveau d'être piratés, provoquant l'inquiétude et la colère des personnels qui paient les conséquences de cette situation.

Dans plusieurs académies, plus aucune application ne fonctionne : messageries professionnelles, outils de gestion des personnels et des élèves… Le versement des salaires pourra-t-il être assuré normalement ? Dans quelles conditions vont être affectés les personnels remplaçants, les contractuels ? Quelle est l'ampleur exacte de la fuite des données personnelles ?

La succession des cyberattaques ayant frappé les systèmes d'information de l'Éducation nationale depuis le début de l'année 2026, Compas en mars, ÉduConnect en avril, SI Formation en juillet, culminant mi-août avec la fuite massive de plus de 346 millions de lignes de données brutes issues de 33 académies et couvrant jusqu'à 20 ans d'archives, n'est plus un incident isolé mais le signe d'une inacceptable défaillance structurelle de la capacité du ministère à garantir la sécurité des données qu'il collecte, tant pour ses agents que pour les usagers du service public d'éducation.

Face à cette situation, le ministère a certes déposé plainte, saisi l'ANSSI ainsi que la CNIL. Si c'est le minimum que l'on puisse attendre, ces actions interviennent après coup, alors que le point d'entrée commun à ces intrusions — un compte ou un accès professionnel détourné — révèle une faiblesse structurelle de l'authentification, et non un simple concours de circonstances. Depuis 2017, les infractions d'atteinte aux systèmes de traitement automatisé de données ont augmenté de 2 700 % au niveau national : le ministère ne pouvait ignorer l'ampleur de la menace.

Cette situation inquiète, et rompt leur confiance des agents avec l'institution qui est légalement responsable de leur protection physique, morale et numérique.

Les données exposées couvrent l'identité, le numéro de sécurité sociale, l'adresse postale, le téléphone, le statut et les fonctions de millions d'agents ayant exercé depuis 2001. Ces informations, une fois diffusées, ne peuvent être « réinitialisées » comme un mot de passe : elles exposent durablement les agents à l'usurpation d'identité administrative, notamment à des tentatives de fraude ciblant la paie, les demandes de mutation ou les dossiers de carrière, un escroc disposant de données exactes et vérifiées étant en mesure de se faire passer pour un service RH légitime. La compromission d'un compte professionnel comme porte d'entrée de l'attaque de juillet doit conduire à un audit complet de l'authentification des messageries professionnelles et des accès aux applications de gestion des ressources humaines (I-Prof et systèmes académiques).

… / …

Nous sommes particulièrement préoccupés par la situation des personnels contractuels, dont les données figurent dans les mêmes bases que celles des titulaires sans que ces agents bénéficient des mêmes garanties statutaires. Contrairement aux fonctionnaires titulaires, les contractuels n'ont ni la sécurité de l'emploi ni, souvent, l'accès aisé aux mêmes canaux d'information et de recours syndical en cas d'usurpation d'identité ou de fraude liée à leur contrat. Un contractuel dont les données administratives sont compromises est plus exposé à la précarisation de sa situation : renouvellement de contrat menacé par une fraude documentaire, difficulté à faire valoir ses droits face à un rectorat en cas de litige lié à une usurpation. Le ministère doit préciser, catégorie par catégorie, l'ampleur de l'exposition des contractuels et mettre en place un accompagnement spécifique.

Le système directement visé par l'intrusion de juillet est aussi celui de la formation des personnels, qui accueille non seulement les stagiaires titulaires mais aussi les contractuels alternants et les étudiants en immersion ou en pratique accompagnée inscrits en master MEEF via les INSPE. Ces publics, souvent très jeunes et en tout début de parcours professionnel, n'ont pas choisi de voir leurs données personnelles engagées dans un système ministériel et n'ont, pour la plupart, aucune connaissance des démarches à entreprendre en cas d'usurpation. Le ministère doit informer individuellement et sans délai tous les étudiants et stagiaires concernés, et qu'il leur garantisse un accompagnement identique à celui des agents titulaires, alors même qu'ils ne sont pas encore fonctionnaires.

Au-delà du seul vol de données déjà préoccupant — environ 1,22 million d'élèves de primaire, de collège et de lycée concernés, avec des données d'identité, de naissance, d'adresse mais aussi des données scolaires et disciplinaires —, il y a un risque d'atteinte à l'intégrité même des systèmes de notation et de vie scolaire. Une intrusion dans un espace numérique de travail ou dans ÉduConnect ne se limite pas à l'exfiltration de données : elle pose la question de la fiabilité des bulletins, des livrets scolaires, de l'attribution des diplômes, des procédures automatisées d'orientation comme Affelnet, et, *in fine*, de la confiance dans l'institution scolaire. Le ministère doit garantir publiquement l'intégrité, la robustesse et la traçabilité de ces données.

Ces fuites successives concernent également les parents et responsables légaux. Si le ministère a déclaré qu'aucune donnée bancaire ni aucun mot de passe n'avait été compromis lors de l'incident de juillet, cette assurance ne couvre pas l'ensemble du périmètre révélé en août, dont le contenu exact reste flou pour les familles. Les procédures de bourses reposent sur des croisements de données fiscales et familiales de plus en plus automatisés notamment pour l'attribution des bourses : toute compromission de ces informations expose les familles à des tentatives de phishing d'autant plus crédibles qu'elles s'appuient sur des données réelles, dans un contexte de rentrée scolaire où les échanges légitimes avec les établissements se multiplient déjà (ENT, cantine, assurance scolaire, fournitures).

Sur le terrain, ce sont les personnels de direction et les personnels administratifs qui doivent assumer, en première ligne et sans moyens supplémentaires, les conséquences opérationnelles de ces piratages : campagnes de réinitialisation de mots de passe en urgence, interruptions de l'espace numérique de travail, blocage de la vie scolaire et des outils de communication avec les familles, et gestion de la communication de crise locale — alors que la décision et la responsabilité technique de ces systèmes échappent totalement à l'établissement puisque partagé entre les collectivités locales et l'État. Des campagnes de sensibilisation ministérielles existent déjà, mais qu'elles ne sauraient se substituer à une sécurisation effective des infrastructures centrales : ce n'est pas aux personnels de compenser, par la pédagogie et la vigilance individuelle, les manquements structurels de sécurité informatique du ministère.

La situation est grave et préoccupante, en réponse, le ministère doit à ses personnels, ses élèves et leurs familles :

… / …

- Une transparence totale et immédiate — communication publique et détaillée, catégorie par catégorie (titulaires, contractuels, stagiaires, étudiants, élèves, parents), du périmètre exact des données compromises lors de chacun des incidents de 2026, sans attendre les conclusions de la CNIL.
- Une information individuelle systématique — notification personnelle de chaque agent, contractuel, étudiant, parent et élève majeur dont les données ont été exposées, avec indication précise de la nature des données concernées, conformément aux obligations du RGPD.
- Un audit indépendant et plan d'urgence — audit de sécurité indépendant de l'ensemble des systèmes d'information du ministère (I-Prof, SCOPE, Compas, ÉduConnect, systèmes de formation académiques), avec calendrier public de mise en œuvre de l'authentification multifacteur généralisée pour tous les comptes professionnels et académiques.
- Une protection spécifique des personnels contractuels — mise en place d'un dispositif d'accompagnement dédié aux agents contractuels, garantissant qu'aucune fraude liée à l'usurpation de leurs données ne puisse être opposée au renouvellement de leur contrat ou à l'exercice de leurs droits.
- Des garanties pour les étudiants et stagiaires en formation — extension explicite à tous les étudiants et stagiaires des INSPE des mêmes droits à l'information et à l'accompagnement que les agents titulaires, alors que leurs données ont transité par les systèmes ministériels de formation.
- Des moyens humains et budgétaires pour les établissements — dotation des établissements en assistance technique de proximité pour la gestion des incidents (réinitialisation de mots de passe, continuité de l'ENT), sans reporter cette charge sur les personnels notamment les personnels de direction ni la publication d'un nouveau vadémécum ou de fiches.
- Aucune sanction contre les agents victimes — engagement écrit qu'aucune conséquence disciplinaire ou administrative ne pourra être tirée contre un agent, un contractuel ou un étudiant victime d'une usurpation d'identité rendue possible par la défaillance des systèmes ministériels.

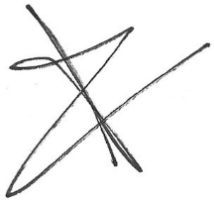
Nous demandons également le rétablissement immédiat des accès aux outils professionnels nécessaires au fonctionnement des écoles, des établissements et des services.

La protection des données personnelles des agents et des usagers constitue une obligation de l'employeur, et non une variable d'ajustement budgétaire. La répétition des incidents en 2026 démontre que les mesures prises jusqu'ici sont manifestement insuffisantes et mettent en danger un système déjà fragilisé par une décade de retraits de moyens, de réorganisation et d'attrition budgétaires. Dans le même temps votre gouvernement a fait voter une augmentation des dépenses militaires de 40 milliards cette année, mais est incapable de donner à nos agences de lutte contre la cybercriminalité les moyens nécessaires.

Nous n'accepterons pas que les agents soient tenus pour responsables de cette situation.

Monsieur le Ministre, prenez les décisions nécessaires pour que cesse cette situation. Nous attendons des actes et non des paroles et encore moins des « postures ».
Nous rappelons que nous avons déposé un préavis de grève qui couvre les différentes catégories de personnels de l'Éducation nationale qui seraient amenées à décider la grève à la rentrée pour obtenir leurs revendications.

Je vous prie de croire, Monsieur le Ministre, à l'assurance de ma parfaite considération.



Clément Poullet, secrétaire général de la FNEC FP-FO