

Annexe 6. Email, internet et médias sociaux

Nous évoluons de plus en plus vers une ère numérique. Comme tous les membres du personnel utilisent chaque jour l'internet, l'e-mail et les médias sociaux, il importe de fixer de bonnes directives régissant l'usage des technologies précitées.

Dans ce contexte, nous renvoyons aux politiques et aux directives sur l'utilisation de l'e-mail, de l'internet et des médias sociaux. La présente annexe porte uniquement sur les principales obligations et modalités de contrôle relatives à l'e-mail et à l'internet.

Le règlement a été rédigé conformément aux dispositions de la convention collective de travail n° 81 et au Règlement général sur la protection des données.

1) Champ d'application

La présente politique s'applique à tous les travailleurs de Renewi, en ce qui concerne:

- les adresses e-mail mises à disposition par Renewi;
- l'accès à l'internet fourni par Renewi; et
- l'utilisation des médias sociaux.

2) Utilisation de l'e-mail

Les adresses et le système e-mail mis à disposition par Renewi sont essentiellement destinés à un usage professionnel. Toutefois, les travailleurs sont autorisés à utiliser, de façon limitée, leur adresse e-mail professionnelle aux fins privées. Il incombe aux travailleurs de classer les e-mails concernés sous la rubrique « privé ». Inversement, les travailleurs ne sont pas autorisés à employer leur adresse e-mail privée aux fins professionnelles.

Les travailleurs ne sont pas autorisés à confier l'accès ou l'usage de leur adresse e-mail professionnelle à des tiers.

Il est strictement interdit d'utiliser l'e-mail pour:

- diffuser des données confidentielles sur l'entreprise (à moins qu'une telle diffusion soit requise dans le cadre du travail);
- diffuser des données violant les droits d'auteur;
- diffuser ou transmettre des messages enfreignant la dignité d'autrui;
- envoyer ou transmettre des messages contraires à l'ordre public et aux bonnes mœurs;
- participer à des chaînes d'emails;
- exercer une activité professionnelle étrangère à l'entreprise;
- exécuter des activités ou des actes de nature illégale.

Les travailleurs doivent respecter la confidentialité de la communication électronique d'autrui et il leur est interdit d'accéder de mauvaise foi aux messages électroniques d'autres travailleurs ou de tiers, et il leur est également interdit de lire les messages précités sans autorisation préalable à cet effet.

Les travailleurs doivent respecter toutes les règles de sécurité informatique et suivre les instructions des services informatiques en la matière.

3) Utilisation de l'internet

L'accès à l'internet est destiné à l'usage professionnel.

L'utilisation aux fins privées est tolérée dans les limites suivantes:

- exclusivement pendant les pauses;
- uniquement pour consulter des sites web généraux (notamment les journaux en ligne, les sites météorologiques, les transports en commun, les informations sur la circulation) au contenu licite.

Il est strictement interdit d'utiliser l'internet (professionnellement ou à titre privé) pour:

- consulter des sites web au contenu illicite;
- consulter des sites de jeux en ligne;
- consulter des sites web dont l'accès est payant et qui exigent une inscription (excepté les sites web professionnels auxquels l'employeur s'est inscrit);
- consulter et participer à des forums de discussion, à des blogs (excepté les forums professionnels auxquels l'employeur souhaite participer);



- télécharger illégalement des données protégées par un droit d'auteur;
- communiquer son adresse e-mail professionnelle sur les sites web visités;
- télécharger des programmes, de la musique ou autres (excepté les téléchargements à partir de sites web professionnels auxquels l'employeur s'est inscrit et qui permettent ces téléchargements).

La liste ci-dessus n'est pas limitative.

4) Utilisation des médias sociaux

L'accès aux médias sociaux et l'utilisation de ceux-ci au travail relève toujours du pouvoir décisionnel exclusif de l'employeur.

L'entreprise préfère cependant tirer avantage des médias sociaux à divers égards. Les médias sociaux peuvent servir, par exemple, à renforcer l'image de marque, mais également à établir des contacts avec des clients et des travailleurs potentiels.

Par ailleurs, les médias sociaux permettent de partager des connaissances et des informations sur les activités de l'entreprise avec les travailleurs, les fournisseurs et les clients. De plus en plus, les médias sociaux participent à la création de l'image de marque de l'entreprise.

En outre, l'entreprise préfère se manifester à l'extérieur sous un seul nom de marque, ce qui explique l'interdiction de comptes secondaires.

Les règles de base suivantes seront respectées:

- Toujours respecter les règles générales de conduite de l'entreprise, qui s'appliquent également aux médias sociaux.
- Respecter les droits d'auteur, ne pas utiliser de documents d'autrui sans leur autorisation, indiquer les sources éventuelles;
- Ne pas dire du mal au sujet de partenaires, de concurrents ou de l'entreprise;
- Ne jamais diffuser d'informations internes (de l'entreprise);
- Ne jamais utiliser le nom ou le logo de l'entreprise dans le nom ou la photo de votre profil;
- Absolument s'abstenir de créer quelque profil sous le nom de l'entreprise, même pas pour des projets bien déterminés;
- Ne jamais agir en tant que porte-parole de votre employeur;
- Ne pas citer les propos de collègues, ni utiliser leurs documents sans autorisation;
- Ne pas publier de messages publicitaires cachés ou de spam;
- Ne jamais réagir aux questions juridiques ou aux situations de crise (dont les accidents ou les incendies), mais en aviser votre supérieur hiérarchique;
- Ne pas diffuser de messages enfreignant la dignité d'autrui.

5) Modalités de contrôle de l'e-mail et de l'internet

a) Finalités du contrôle

L'employeur a le droit de contrôler l'usage, par ses travailleurs, des ressources mises à leur disposition.

L'employeur procède au contrôle de l'utilisation de l'e-mail et de l'internet pour:

- éviter les faits illégaux ou diffamatoires, les faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autres personnes;

Il s'agit notamment des faits suivants: le piratage informatique, la consultation de sites pornographiques ou pédophiles, voire de sites incitant à la discrimination, à la ségrégation raciale, à la haine ou à la violence contre un groupe, une communauté ou les membres de ceux-ci, pour cause de race, de couleur de la peau, d'origine, d'ascendance religieuse, nationale ou ethnique des membres de tels groupes ou communautés, voire de certains membres de ceux-ci.

- protéger les intérêts économiques, commerciaux et financiers de l'entreprise qui sont de nature confidentielle et lutter contre les pratiques qui y sont contraires;

Il s'agit notamment de certains actes de publicité négative, de la diffusion de fichiers et de la violation de secrets d'affaires, y compris la recherche et le développement, les procédés de production et toutes les données confidentielles imaginables.

- assurer ou rétablir la sécurité et/ou le bon fonctionnement technique des systèmes de réseau informatique de l'entreprise, y compris le contrôle des frais y afférents, ainsi que la protection physique des installations de l'entreprise;

Il s'agit notamment d'éviter ou de résoudre la surcharge du réseau ou le diffusion de virus.

- Veiller au respect, de bonne foi, des principes et des règles en vigueur au sein de l'entreprise régissant l'utilisation des technologies en ligne.

b) Proportionnalité

En principe, le contrôle des données électroniques de communication en ligne ne peut pas entraîner une ingérence dans la vie privée des travailleurs. Si le contrôle donne malgré tout lieu à une ingérence dans la vie privée d'un travailleur, l'ingérence sera limitée au minimum.

c) Contrôle global

Un contrôle global peut intervenir à tout moment. Par sa nature globale, le contrôle comprend:

- la collecte du nombre d'e-mails reçus ou envoyés par poste de travail, le suivi du volume des e-mails et du format des documents joints;
- le relevé des sites web visités, du moment de la connexion et de la durée de la connexion.

6) Suivi du contrôle de l'utilisation de l'e-mail et de l'internet: procédure à la constatation d'une irrégularité

a) Individualisation directe et indirecte

Lorsque l'employeur constate une irrégularité suite à un contrôle global, il procède à l'individualisation des données en vue d'identifier le travailleur responsable de l'irrégularité.

- **L'individualisation est directe** quand le contrôle global a pour objet:
 - éviter les faits illégaux ou diffamatoires, les faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autres personnes;
 - protéger les intérêts économiques, commerciaux et financiers de l'entreprise qui sont de nature confidentielle et lutter contre les pratiques qui y sont contraires;
 - assurer ou rétablir la sécurité et/ou le bon fonctionnement technique des systèmes de réseau informatique de l'entreprise, y compris le contrôle des frais y afférents, ainsi que la protection physique des installations de l'entreprise.

L'individualisation directe signifie que l'employeur procède à l'identification du travailleur responsable de l'irrégularité, sans le moindre avertissement préalable.

- **L'individualisation est indirecte** quand le contrôle global a pour objet de vérifier si les travailleurs respectent les dispositions du présent règlement.

Dans ce cas, l'employeur avertit les travailleurs que des irrégularités ont été constatées au cours d'un contrôle global et que les données seront individualisées si l'employeur constate que de telles irrégularités se sont reproduites.

Lorsque l'employeur souhaite sanctionner un travailleur ayant commis l'irrégularité, il l'invitera à un entretien préalable, de sorte que le travailleur pourra y donner des explications sur son usage de l'e-mail et de l'internet.

L'entretien ne sera pas organisé si le contrat de travail du travailleur est suspendu pour quelque motif à la constatation des faits.

b) Droits et obligations des personnes chargées du contrôle

Les personnes compétentes pour exécuter le contrôle **est le HR Director** en collaboration avec le responsable du service informatique.

Ces personnes sont compétentes pour:

- exécuter ou faire exécuter le contrôle global par le responsable du service informatique;
- évaluer s'il convient de procéder à l'individualisation directe ou indirecte;
- informer les travailleurs des mesures à prendre à la réception d'e-mails suspects ou en prenant connaissance de choses suspectes sur les sites web consultés;
- mener l'entretien préalable avec le travailleur suite à un contrôle. Le travailleur concerné peut se faire assister par un représentant de la délégation syndicale.

c) Conserver les données à caractère privé

Les données à caractère privé collectées à l'occasion d'un contrôle seront conservées pendant une période de douze mois au service informatique.

Le travailleur a le droit de prendre connaissance de ses données à caractère privé collectées lors du contrôle et de prier éventuellement l'employeur de modifier ou d'effacer les données éventuellement erronées.

7) Sanctions

Le travailleur ne respectant pas les données du règlement pourra se voir infliger une des sanctions mentionnées dans le règlement de travail.

Lorsque le travailleur enfreint le règlement à plusieurs reprises, qu'il commet une infraction grave ou que ses actions portent préjudice à l'employeur, il pourra être licencié pour motif grave, sans préavis ni indemnité.

8) Information (transparence)

Ce règlement a été élaboré après consultation du comité d'entreprise et figure en annexe du règlement du travail.