Conseil départemental de l'Hérault
Direction de la Lecture publique départementale

Guide des bonnes pratiques numériques

Voté le 15 mai 2023, le Schéma de Développement de la Lecture publique départementale (2023-2028) a pour ambition de développer l'offre de lecture publique sur le territoire autour de trois grands axes structurants : l'équité, l'inclusion et l'expertise.

Depuis des années, la Direction de la Lecture publique s'engage dans l'accès à la culture numérique pour tous et toutes, en zones rurales, conformément au Plan Bibliothèque d'avril 2018 et à la Loi Robert du 21 décembre 2021.

Issu du Schéma, le Groupe de travail Numérique vous présente la Charte des bonnes pratiques numériques, élaborée en 2023. Ce texte formalise un ensemble de bonnes pratiques du numérique en bibliothèque. Conçu comme un outil pour tous les professionnels de la lecture publique, il s'accompagne d'un glossaire et d'une sitographie.

Table des matières

Agir en conformité avec la législation française et européenne

La législation relative au numérique n'a cessée d'évoluer au cours des dernières années, notamment avec l'introduction du RGPD (ou Règlement Général sur la Protection des Données). Dans nos métiers, il est essentiel d'appliquer au mieux les différentes réglementations françaises ou européennes, tant dans nos pratiques professionnelles qu'auprès de nos publics.

1. Législation française

En France, l'informatique et les usages du numérique sont encadrés par la loi. Si certaines de ces lois sont propres au numérique, d'autres sont transposables, notamment celles qui relèvent des droits et des libertés individuelles.

- Mettre en place des conditions propices au respect des libertés individuelles
- Garantir et agir pour le respect de la propriété intellectuelle, conformément au code de la propriété intellectuelle
- Garantir le respect de la licence Creative Commons
- Garantir le respect du droit à l'image
- Garantir le respect de l'e-identité des usagers
- Garantir un accès sûr et sécurisé à internet pour tous dans le respect des législations en cours
- Veiller à ce que l'usage qui est fait de cet accès réponde aux obligations légales concernant :
    - La protection des mineurs (Code pénal, articles 227-23 et 227-24)
    - La fraude informatique (loi Godfrain du 5 janvier 1988)
    - La conservation des données de trafic (loi Vaillant du 15 novembre 2001 et loi du 23 janvier 2006 relative à la lutte contre le terrorisme)
- S'assurer que la conservation des données personnelles des usagers soit conforme :
    - A la loi Informatique et liberté du 6 janvier 1978
    - A la loi n° 2006-64 du 23 janvier 2006
    - Au décret 2006-358 du 24 mars 2006
    - A la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- Garantir le respect de la loi n°2021-1485, dite REEN (Réduire l'Empreinte Environnementale du Numérique) du 15 novembre 2021

2. Règlement Général sur la Protection des Données (RGPD)

Le Règlement Général sur la Protection des Données est un règlement européen. Il encadre la collecte et le traitement des données personnelles des citoyens, sur l'ensemble du territoire de l'Union européenne.

- S'assurer que la Collectivité dont on dépend dispose d'un délégué à la protection des données (DPO) ou d'une délégation dédiée

- S’assurer que toute collecte de données personnelles des usagers est précédée d’un enregistrement au Registre des Traitements de Données Personnelles
- Limiter la collecte aux seules données strictement nécessaires, pour un but précis et légitime, nécessaire à la réalisation d’un objectif
- Ne pas traiter les données d’une manière qui serait incompatible avec l’objectif initial
- Limiter la manière dont les données personnelles de l’usager seront utilisées et réutilisées
- Fixer des durées de conservation pour ne conserver les données personnelles des usagers que le temps strictement nécessaire à l’objectif poursuivi
- Détruire, anonymiser ou archiver les données personnelles des usagers dans le respect des obligations légales une fois que la durée de conservation établie est écoulée
- Garantir la sécurité des données personnelles des usagers
- Adapter les mesures de sécurité en fonction de la sensibilité des données ou des risques qui peuvent peser sur les personnes en cas d’incident de sécurité
- S’assurer que seul le personnel légalement autorisé a accès aux données
- Être transparent quant à la collecte et à l’utilisation des données personnelles des usagers :
    - Ne pas collecter les données personnelles des usagers à leur insu
    - Informer clairement et systématiquement les usagers, dès le moment ou des données sont collectées, sur leurs droits et devoirs, ainsi que l’usage qui en sera fait
- Respecter le droit des usagers quant au traitement de leur données personnelles
- Ne pas diffuser les données personnelles des usagers sans leur consentement libre, spécifique, éclairé et univoque (par exemple, il est interdit de communiquer un mail ou un numéro de téléphone à un tiers, sans le consentement exprès de l’usager, y compris dans le cas d’une demande émise par une association ou autre pour obtenir une liste de diffusion)
- Inscrire la mise en conformité dans une démarche continue
    - Vérifier régulièrement que la règlementation n’a pas évolué
    - Vérifier que les procédures et les mesures de sécurité mises en place sont bien respectées et les adapter si cela s’avère nécessaire
    - Être attentif au respect du cadre légal dans ses tâches quotidiennes
- Se former et s’informer quant au cadre légal sur les données personnelles.

Assurer la cybersécurité

La cybersécurité regroupe l’ensemble des moyens que l’on peut mettre en œuvre afin d’assurer la sécurité des systèmes et des données informatiques. Elle permet de prévenir les différentes menaces et attaques (piratage, virus, usurpation d’identité, etc.) pour préserver à la fois votre matériel, la confidentialité et l’intégrité de vos données et/ou celles de vos usagers, la vie privée et les libertés. En bibliothèque, il est essentiel de mettre en œuvre les moyens techniques de cybersécurité mais aussi de sensibiliser les utilisateurs aux risques et aux bonnes pratiques.

Règle d'or

Ne jamais laisser un ordinateur connecté à une session ou un compte personnel sans surveillance. Verrouiller la session (touches « windows » + L) ou se déconnecter systématiquement en cas d'absence.

1. Les mots de passe

- Utiliser un mot de passe différent pour chaque site web, service ou réseaux
- Construire des mots de passe longs et complexes. Un bon mot de passe doit contenir 12 caractères, dont des majuscules, des minuscules, des chiffres et des caractères spéciaux. Les informations personnelles telles que la date de naissance, le département ou les noms d'animaux sont à éviter
- Ne jamais communiquer ses mots de passe
- Ne pas enregistrer vos mots de passe sur votre navigateur ou un ordinateur partagé
- Activer la double identification dès que cela est possible
- Utiliser un gestionnaire de mot de passe comme « keepass » pour conserver vos mots de passe
- Au moindre soupçon, il est nécessaire de changer l'ensemble de vos mots de passe

2. Les mises à jour

- Penser à mettre à jour régulièrement l'ensemble de vos appareils et logiciels : pour cela, vous pouvez activer l'option de téléchargement et d'installation automatique des mises à jour et les planifier lors de périodes d'inactivité
- Se méfier des fausses mises à jour sur internet (par exemple lorsqu'une fenêtre pop-up vous alerte, etc.), télécharger les mises à jour uniquement depuis les sites officiels
- Protéger autrement les appareils qui ne peuvent pas être mis à jour (supprimer la connexion internet, désactiver les services, applications vulnérables…)

3. Les sauvegardes

- Identifier les appareils et supports qui contiennent des données et déterminer celles devant être sauvegardées
- Choisissez une solution de sauvegarde adaptée à vos besoins (support physique, virtuel)
- Effectuer et planifier des sauvegardes régulières de vos données
- Faire une sauvegarde avant d'installer une mise à jour
- Déconnecter votre support de sauvegarde après utilisation

- Protéger et tester vos sauvegardes

4. Antivirus et pare-feu

- Munissez-vous d'un ou plusieurs antivirus pour vous protéger des attaques malveillantes
- Pensez à mettre à jour régulièrement votre antivirus
- Procédez régulièrement à des analyses (dit scans), y compris du support de sauvegarde

5. Internet

- Eviter les connexions wi-fi publics ou inconnues. Le cas échéant, ne jamais réaliser d'opérations sensibles en étant connecté à un wi-fi public (consultation de comptes bancaires, achats en ligne, mail personnels et/ou professionnels…)
- Vérifier systématiquement la fiabilité d'un site (présence du http**s** ; cadenas)
- Télécharger et installer des logiciels et des applications uniquement depuis les sites officiels
- Sur les sites marchands, privilégier un moyen de paiement sécurisé et tiers de confiance comme les solutions « paylib » ou « paypal »
- Vérifier systématiquement l'usages des données collectées sur les sites et/ou logiciels
- Eviter d'accepter le dépôt de cookies lors de la consultation d'un site, paramétrer la gestion des cookies dans votre ordinateur, supprimer régulièrement votre historique
- Se munir d'un bloqueur de publicité comme « adblock » ou « ublock origine »

6. Les réseaux sociaux

- Vérifier régulièrement les connexions aux comptes
- Eviter d'utiliser un compte de réseau social pour s'authentifier sur d'autres sites (se connecter avec google, facebook...)
- Contrôler les paramètres de confidentialité des comptes, ainsi que les applications tierces et les autorisations
- Maîtriser vos publications pour préserver votre e-réputation
- Ne pas diffuser ou communiquer à une personne inconnue vos informations personnelles (adresse, numéro de téléphone, etc.)
- Faire attention aux fausses informations et offres qui circulent librement sur les réseaux sociaux. Penser à toujours vérifier leur source

7. Vie professionnelle et vie personnelle

- Préserver votre vie privée :

- Ne pas utiliser les mêmes matériels informatiques, logiciels, mots de passe, adresse mail et numéro de téléphone dans la vie privée et la vie professionnelle
- Reconnaître, appliquer et faire valoir le droit à la déconnexion : ne pas utiliser les outils de communication professionnels en dehors des heures de bureaux (soirées, week-end, congés)

- Préserver votre santé physique et mentale :
  - Organiser son temps de travail pour gérer les informations reçues par voie électronique (mail, sms, etc…)
  - Garder la maîtrise de votre identité numérique (e-réputation : modérer ses propos, le contenu publié, préserver son intimité)
  - Adapter votre environnement numérique de travail afin d'avoir une bonne posture devant les écrans et un confort visuel et cognitif. Si besoin, faites appel à un ergothérapeute
  - Faire des pauses visuelles (quitter fréquemment l'écran des yeux quelques secondes), bouger régulièrement (se lever, s'étirer, marcher)

Enfin, ne pas oublier de sécuriser l'ensemble de vos appareils : téléphone portable, montre connectée (…), de la même façon que votre ordinateur. Tout matériel numérique doit être protégé.

Adopter un numérique sobre et écoresponsable

Dans le contexte actuel de transition écologique, il est essentiel de prendre en compte les répercussions environnementales du numérique. En France, la pollution numérique représenterait 2,5 % de l'empreinte carbone nationale et 20 millions de tonnes de déchets par an, soit 299 kg par habitant. La fabrication des outils informatiques constituerait 78 % de cette pollution, tandis que la phase d'usage s'élèverait à 21 %. Afin de réduire l'impact du numérique sur l'environnement, il existe des gestes et des pratiques simples à mettre en place au quotidien.

1. Les équipements informatiques

- S'équiper sobre en se fiant aux écolabels EPEAT et TCO, ou acheter des appareils reconditionnés
- Prendre en compte l'indice de réparabilité et la consommation énergétique d'un appareil lors d'une acquisition
- Limiter le renouvellement des équipements numériques au strict nécessaire
- Réparer et allonger la durée de vie des appareils
- Utiliser des logiciels dits « libres », moins gourmands en ressources afin de préserver les machines et allonger leur durée de vie.
- Mutualiser au maximum les équipements professionnels ou à destination des publics.

2. Flux et stockage de données

- Internet et stockage :
    - Optimiser sa navigation avec des raccourcis
    - Favoriser la lecture en ligne plutôt que l'impression ou le téléchargement lorsque que le temps de lecture est inférieur à deux minutes
    - Ne télécharger en ligne que les documents nécessaires ou fréquemment consultés
    - Désactiver la synchronisation automatique entre vos matériels fixes et mobiles. Celle-ci augmente la consommation d'énergie et génère un flux de données continu
    - Eviter d'archiver sur des clouds et favoriser un stockage en local des documents, à condition d'avoir prévu un dispositif de sauvegarde. Contrairement aux clouds, le local ne génère pas de flux de données

- Boîte mail et visioconférences :
    - Limiter les échanges de mails à son minimum : ne pas faire « répondre à tous » systématiquement, se déplacer pour échanger de vive voix, passer un appel téléphonique, limiter les réponses automatiques
    - Limiter et compresser les données échangées : pièces jointes, images, signatures… Si possible, partager un lien vers un répertoire partagé ou une GED ou une plateforme d'échanges sécurisés
    - Favoriser les réunions en présentiel lorsque cela est possible et que cela ne conduit pas à une utilisation massive et/ou sur une grande distance de véhicules polluants
    - N'activer la caméra en visioconférences que pour vous présenter, durant vos prises de paroles ou lorsque cela est vraiment nécessaire. En effet, la vidéo génère 1 000 fois plus de flux de données que l'audio seul. Une minute de visio-conférence émet 1g de CO2 (Leboucq, 2020)

3. Consommation énergétique

- Adapter la luminosité des écrans
- Mettre en veille vos appareils pour toute inactivité de moins de quinze minutes
- Eteindre les appareils plutôt que de laisser en veille pour toute absence de plus de quinze minutes
- Eteindre l'ensemble de vos appareils en quittant votre poste de travail à la fin de la journée
- Si possible, utiliser des multiprises avec un interrupteur afin de stopper toute conduction d'électricité lors de votre absence

4. L'impression

- Limiter les impressions qui favorisent les flux de données et privilégier l'impression depuis une clé USB, préalablement analysée par l'antivirus de votre poste, interne à la bibliothèque et n'appartenant pas au public (source potentielle de virus). Penser à reformater la clef USB après chaque utilisation

- Privilégier les photocopies, moins gourmandes en données, plutôt que les impressions multiples
- Régler vos paramètres d'impression pour :
    - Imprimer en recto-verso
    - Imprimer en noir et blanc
    - Utiliser la fonction permettant d'économiser l'encre
- Privilégier les polices de caractères économes et préservant le confort de lecture telles que :
    - Times New Roman, taille 11
    - Arial, taille 10
    - Cambria, taille 11
    - Calibri, taille 11

5. Service en ligne

- Evaluer régulièrement l'empreinte carbone de son portail avec l'outil « GT metrix »
- Se limiter aux besoins réels des utilisateurs et supprimer les fonctionnalités inutiles
- Rendre le parcours utilisateur plus simple et efficace pour limiter les flux
- S'assurer que le site est web-responsive et s'adapte à tout type d'écran et d'équipement
- Gérer et limiter le poids des contenus en ligne : compresser les pdf, limiter les feuilletoirs et les vidéos au nécessaire, bloquer leur lecture automatique et paramétrer leur résolution afin d'éviter la très haute définition, trop gourmande en ressources

6. Proposer aux usagers des services en faveur d'un numérique sobre et responsable

- Proposer un wifi ouvert et gratuit afin de limiter l'usage de la 4G
- Equiper les postes publics en logiciels libres
- Faire du prêt de matériel numérique pour éviter le suréquipement individuel (liseuses, tablettes…)

Accompagner les publics

1. Permettre l'accès pour tous et toutes au numérique

- Garantir la gratuité
- Garantir la neutralité, l'impartialité et l'inclusivité
- Mettre à disposition des infrastructures et des équipements adaptés (ordinateur, connexion wifi…) et sécurisés.

- Mettre à disposition des ressources de formation au numérique : bibliographies, tutos, capsules vidéo, ressources en ligne, etc.
- Adapter les équipements et les ressources pour tous et toutes : dys, handicaps, allophones, etc.

2. Informer et sensibiliser

- Connaître son territoire et les acteurs du numérique afin de rediriger vers les structures adéquates (France Service, etc.) et/ou travailler en partenariat
- Informer et communiquer sur les ressources disponibles
- Accompagner les publics dans leurs pratiques et leurs connaissances du numérique en favorisant une médiation ludique
- Mettre en place des actions (ateliers, animations, expositions, conférences, etc.) en faveur de la culture numérique :
    - Informer, sensibiliser et former aux outils, aux bonnes pratiques et aux usages numériques
    - Informer et sensibiliser sur les données personnelles, le cadre juridique, les droits et les devoirs des citoyens et citoyennes
    - Informer et sensibiliser sur la cybersécurité, les risques et comment s'en prémunir
- Mettre en place des ressources et des actions (ateliers, animations, expositions, conférences, etc.) en faveur de l'Education aux Médias et à l'Information (EMI) :
    - Informer et sensibiliser sur la désinformation et les fakes news
    - Sensibiliser et former les publics à la recherche et à la vérification des sources d'informations
    - Sensibiliser et former aux différents médias (radio, presse, internet…) et aux réseaux sociaux (Instagram, youtube, etc.)
    - Sensibiliser et former à l'esprit critique
- Mettre en place des ressources et des actions (ateliers, animations, expositions, conférences, etc.) en faveur de la parentalité numérique :
    - Informer et sensibiliser sur les activités numériques des enfants et adolescents, leurs pratiques et usages du numérique, ainsi que les outils utilisés
    - Informer et sensibiliser sur les différents risques et problématiques auxquelles les enfants et les adolescents peuvent être confrontés (cyberharcèlement, accès à des contenus choquants, illicites ou pornographiques, etc.)

    - Informer et accompagner les parents sur les moyens existants (outils techniques, dialogue, régulation des temps d'écran, etc.) pour accompagner et protéger leurs enfants dans leurs usages du numérique
- Mettre en place des ressources et des actions (ateliers, animations, expositions, conférences, etc.) en faveur d'un numérique sobre et responsable :
    - Informer et sensibiliser sur la pollution numérique, la sobriété et l'écoresponsabilité numérique
    - Sensibiliser et former aux bonnes pratiques en matière d'écoresponsabilité numérique
    - Organiser des « Install Party » ou des « repair cafés » informatiques

Glossaire

Appareils reconditionnés : produit qui a déjà été utilisé, réparé et/ou remis à neuf, commercialisé à nouveau

Clouds : serveurs informatiques permettant de stocker et traiter des données à distance et en réseau sur internet

Cookies : les cookies sont de petits fichiers contenant des informations de navigation (les pages visitées, l'heure, la date, vos préférences, vos comportements, profil d'internaute et de consommateur…)

Données personnelles : les données personnelles correspondent aux informations permettant d'identifier une personne physique directement ou indirectement (nom et prénom, numéro de sécurité sociale, date de naissance, numéro de téléphone…)

Double identification : la double identification ou authentification est une méthode qui permet de renforcer la sécurité d'accès d'un compte utilisateur. L'authentification à double facteur est un processus de sécurité par lequel l'utilisateur fournit deux modes d'identification à partir de catégories de données distinctes : l'une se présente généralement sous la forme d'un jeton physique, comme une carte, et l'autre sous forme d'informations mémorisées, par exemple un code de sécurité. Ces deux facteurs représentent une chose *possédée* et une chose *sue*.

Généralement, en plus de renseigner vos identifiants traditionnels, vous recevez un code à usage unique supplémentaire pour pouvoir accéder à votre compte

DPO : le sigle DPO signifie « Délégué à la Protection des Données ». Un ou une DPO est chargé de mettre en œuvre la conformité au RGDP au sein de sa structure

Ecoresponsable : être écoresponsable, c'est faire preuve de responsabilité vis-à-vis de l'environnement et agir en conséquence, en respectant au maximum l'environnement

Empreinte carbone : l'empreinte carbone est une unité de mesure de la quantité de gaz à effet de serre émise par l'activité humaine

Gestionnaire de mots de passe : logiciel ou service en ligne qui permet à un utilisateur de gérer ses mots de passe en les centralisant dans un espace sécurisé. (Attention ! l'enregistrement des mots de passe sur le navigateur - type google chrome -, ne correspond pas à un service en ligne ou un logiciel sécurisé. Il est déconseillé d'enregistrer les mots de passe sur un navigateur)

Indice de réparabilité : il s'agit d'un indicateur, sous forme de note, qui permet aux consommateurs de connaître les possibilités ou taux de réparation sur un appareil

Licence Creative Commons : les Creative Commons sont un ensemble de licences qui régissent les conditions de réutilisation et de distribution des œuvres

Logiciels libres : programme informatique qui n'a pas de propriétaire. La licence d'un logiciel libre appartient à tout le monde, son code est accessible à tous et à toutes, et peut être utilisé, modifié, dupliqué et diffusé librement

Navigateur : un navigateur est une application qui permet d'accéder à internet

Navigation : action d'utiliser internet à partir d'un navigateur

Paramètres de confidentialité : il s'agit de l'ensemble des paramètres réglables permettant de choisir à qui, quand et comment une ou plusieurs informations sont accessibles

Parcours utilisateurs : il s'agit du parcours, de l'ensemble des étapes suivies par un usager lors de son utilisation d'un service en ligne

Pare-feu : logiciel qui permet de protéger un système informatique connecté à internet des tentatives d'intrusion ou piratage

Pollution numérique : la pollution numérique désigne l'ensemble des impacts environnementaux engendrés par les technologies informatiques, de l'information et de la communication, de leur fabrication jusqu'à leur destruction, en passant par leur utilisation

Pop-up : il s'agit d'une fenêtre flottante, qui s'affiche par-dessus la page internet ouverte

Raccourci : petit fichier qui redirige vers un autre fichier ou site internet

Repair café : un repair café est un atelier dédié à la réparation d'objets, dans un esprit de tiers-lieu

Sauvegarde : opération qui consiste à dupliquer des données informatiques et à les placer en sécurité afin de les conserver

Virus : programme informatique malveillant dont l'objectif est de perturber le bon fonctionnement d'un outil informatique, par exemple en endommageant ou en supprimant des données

Web-responsive : technique qui permet d'adapter un site internet à tous les écrans, quelle que soit leur taille.

Sitographie

Législation française et européenne :

Code de la propriété intellectuelle. 1e juillet 1992. Legifrance.
https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006069414/

Fraude informatique. Loi n°88-5 du 5 janvier 1988. Legifrance.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000875419

Informatique et libertés , loi n°78-17 du 6 janvier 1978. Legifrance.
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

Protection des données personnelles, loi n°2018-493 du 20 juin 2018. Legifrance.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952

Règlement Général sur la protection des données du 27 avril 2016. CNIL.
https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Loi REEN. Loi n°2021-1485 du 15 novembre 2021. Legifrance.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044327272

Droit à l'image :

- Article 226-1 code pénal du 1e mars 1994. Legifrance.
  https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193566
- Article 226-8 code pénal du 1e mars 1994. Legifrance.
- Article 222-33-3 code pénal du 1e mars 1994. Legifrance.
  https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000029336973
- Article 35 quater, loi du 29 juillet 1881. Legifrance.
  https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006419802
- Protéger son droit à l'image. Gouvernement.fr. 21 septembre 2021.
  https://www.gouvernement.fr/guide-victimes/proteger-son-droit-a-l-image#:~:text=L'article%20226%2D8%20du,est%20pas%20express%C3%A9ment%20fait%20mention.

Protection des mineurs :

- Article 227-23 code pénal du 1e mars 1994. Legifrance.
  https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043409170#:~:text=Article%20227%2D23-,Version%20en%20vigueur%20depuis%20le%2023%20avril%202021,75%20000%20euros%20d'amende.
- Articles 227-24 code pénal du 1e mars 1994. Legifrance.
  https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418096/2000-04-13#:~:text=Le%20fait%20soit%20de%20fabriquer,emprisonnement%20et%20de%20500%20000

S'informer et se former sur la législation numérique :

Licences Creatives Commons. Creativecommons.org. https://creativecommons.org/share-your-work/cclicenses/

Commission Nationale de l'Informatique et des Libertés (CNIL). https://www.cnil.fr/fr

Commission Nationale de l'Informatique et des Libertés - *L'atelier RGPD* - https://atelier-rgpd.cnil.fr/login/index.php - Mooc proposé par la CNIL pour se former gratuitement au RGPD.

Cybersécurité, usages et numérique

Cybermalveillance.gouv. https://www.cybermalveillance.gouv.fr/

Openclassroom - *Les bases de la sécurité informatique* - https://openclassrooms.com/fr/courses/5870206-decouvrez-les-bases-de-la-securite-numerique – Module gratuit de e-learning sur la cybersécurité.

Internet sans crainte. https://www.internetsanscrainte.fr/

Cybermalveillance.gouv – *Cyberguide famille* - https://www.cybermalveillance.gouv.fr/medias/2019/11/231025_GuideFamilles_SCREEN.pdf - Guide parents-enfants sur la sécurité numérique.

ADEME – *Caractérisation des effets rebond induits par le télétravail* - https://librairie.ademe.fr/mobilite-et-transport/3776-caracterisation-des-effets-rebond-induits-par-le-teletravail.html - Rapport d'étude sur les effets du télétravail.

Numérique sobre et responsable :

GTmetrix - https://gtmetrix.com/ - Outil pour calculer l'empreinte environnementale d'un site internet.

Electronic Product Environmental Assesment Tool - *Ecolabel EPEAT* - https://www.epeat.net/

TCO certified – *Ecolabel TCO* - https://tcocertified.com/fr/tco-certified/

Francenum.gouv – *10 écogestes numériques responsables* - https://www.francenum.gouv.fr/10-ecogestes-numeriques-responsables - Article et infographie.

Etudes et informations sur l'impact environnemental du numérique :

Cairn.info – Responsabilité et environnement – *Transition numérique et transition écologique* : https://www.cairn.info/revue-responsabilite-et-environnement-2017-3.htm - Ce numéro de Responsabilité et Environnement est entièrement consacré à l'interconnexion entre la transition écologique et la transition numérique.

Green IT – *Empreinte environnementale du numérique mondial* : https://www.greenit.fr/etude-empreinte-environnementale-du-numerique-mondial/#introduction – Etude sur la quantification de l'empreinte du numérique à l'échelle mondiale sur l'environnement et son évolution entre 2010 et 2025.

LeMagIT – *Quelles solutions pour un numérique sobre ?* : https://www.lemagit.fr/tribune/Quelles-solutions-pour-un-numerique-sobre - Article proposant une première approche des termes autour de la sobriété numérique.

Qu'est-ce qu'on fait ? – *Pollution numérique : du clic au déclic* : https://archives.qqf.fr/infographie/69/pollution-numerique-du-clic-au-declic - Infographie sur la consommation d'énergie et de ressources de nos appareils et de leurs usages.

Guides, méthodes et proposition d'actions vers la sobriété numérique :

ADEME Agence de l'environnement et de la maîtrise de l'énergie – *Numérique responsable* : https://communication-responsable.ademe.fr/numerique-responsable - Guide, méthodes et documents pour concevoir et découvrir les bonnes pratiques du numérique responsable.

ADEME Agence de l'environnement et de la maîtrise de l'énergie - *Ecoresponsable au bureau*. https://www.ecologie.gouv.fr/sites/default/files/ecoresponsable_au_bureau-2.pdf – Guide des bonnes pratiques quotidiennes au travail.

Educavox – Sarah Descamps, Gaëtan Temperman et Bruno De Lièvre – *Vers une éducation à la sobriété numérique* : https://www.educavox.fr/accueil/debats/vers-une-education-a-la-sobriete-numerique - Article proposant une réflexion sur la nécessité et les enjeux de l'instauration d'un enseignement obligatoire à l'éducation sur la sobriété numérique.

Institut du Numérique Responsable – *Mooc Numérique Responsable* : https://institutnr.org/mooc-numerique-responsable-complet - Ensemble de modules d'apprentissage pour se former aux bonnes pratiques du numérique.

Ministère de la transition écologique et Direction interministérielle du numérique – *Guide de bonnes pratiques numérique responsable pour les organisations* : https://ecoresponsable.numerique.gouv.fr/publications/bonnes-pratiques/ - Guide pour élaborer un plan d'action pour un numérique responsable au sein d'une organisation privée ou publique.

The Shift Project – *Décarbonons la culture !* : https://theshiftproject.org/article/decarboner-culture-rapport-2021/ - Rapport et synthèse d'un plan pour réduire le bilan carbone du milieu culturel français.

Cu-arras – *Imprimer ? Oui mais éco-responsable* - https://www.cu-arras.fr/wp-content/uploads/2021/04/FichePratique-1.pdf - Fiche pratique sur l'impact environnemental des impressions papier.

Agir en bibliothèque pour un numérique sobre et responsable :

ABF Bibliothèques vertes : https://bib.vertes.abf.asso.fr/ - Blog de la commission Bibliothèques Vertes de l'Association des Bibliothécaires de France qui propose des ressources et des articles sur l'écologie et le développement durable dans les domaines des bibliothèques.

Agenda 2030 et Bibliothèques France – *Un accès et des opportunités pour tous* : https://agenda2030bibfr.wixsite.com/agenda2030bib/brochure - Brochure proposant des exemples concrets de démarches durables à faire en bibliothèque.

Education aux médias et à l'information :

Informations et ressources :

ENSSIB – *EMI* - https://emi.enssib.fr/ - Site d'informations et de ressources.

CLEMI – *Centre pour l'éducation aux médias et à l'information* - https://www.clemi.fr/ - Informations et ressources diverses.

Les promeneurs du Net - https://www.promeneursdunet.fr/ - Actualités, informations et ressources.

B.n.F. – *Ressources pour les enseignants* - https://www.bnf.fr/fr/ressources-pour-les-enseignants - Ensemble de ressources (affiches, expositions).

Cité des sciences et de l'industrie – *Ressources pour l'éducation aux médias* - https://www.cite-sciences.fr/fr/au-programme/lieux-ressources/bibliotheque/se-former-reviser/education-aux-medias/ressources-pour-leducation-aux-medias - Ensemble de ressources pédagogiques.

Cité des sciences et de l'industrie – *Education aux médias et à l'information scientifique* - https://www.cite-sciences.fr/fr/au-programme/lieux-ressources/bibliotheque/se-former-reviser/education-aux-medias - Ressources documentaires et numériques.

ACRIMED – *Médias français : qui possède quoi ?* - https://www.acrimed.org/Medias-francais-qui-possede-quoi - Infographie du paysage médiatique en France.

Hugo Décrypte - https://www.youtube.com/channel/UCAcAnMF0OrCtUep3Y4M-ZPw/videos - Résumé et décryptage de l'actualité quotidienne.

Info ou Mytho - https://www.youtube.com/@InfoouMytho – Chaîne d'esprit critique pour les adolescents.

La série Spam : https://enseignants.lumni.fr/parcours/1237/spam-une-serie-pour-decrypter-les-medias-et-l-information-avec-vos-eleves-emi.html - Série vidéo d'éducation aux médias et à l'information.

Guides et livrets :

Bibliothèque publique d'information – *Education aux médias et à l'information en bibliothèque de lecture publique* - https://www.bpi.fr/content/uploads/sites/3/2020/03/emi-guide-pratique-2020.pdf - Guide pratique de l'EMI en bibliothèque.

Bibliothèque sans frontière - *EMI en bibliothèques* - https://www.bibliosansfrontieres.org/wp-content/uploads/2022/11/Fiches-Animation-EMI-en-bibliotheques-2e-edition-1.pdf - Livret de fiches d'animations.