

SÉQUENCE

D'APPRENTISSAGE

SUR BASE DU PROGRAMME
DU TRONC COMMUN

SECONDAIRE S1



NUMÉRIQUE

**SÉQUENCE 6 : CITOYENNETÉ NUMÉRIQUE -
IDENTITÉ, TRACES ET ÉQUILIBRE DE VIE**



WALLONIE-BRUXELLES
ENSEIGNEMENT

Tronc commun

Citoyenneté numérique : identité, traces et équilibre de vie

1. Généralités

Titre de la séquence	Citoyenneté numérique : identité, traces et équilibre de vie
Année	S1
Discipline	FMTTN – Volet numérique
Champs	Informations et données – Sécurité – Communication et collaboration – Intelligence artificielle

2. Le dispositif amène les élèves à...

Cette séquence amène les élèves à développer une posture de citoyen numérique responsable, capable de comprendre, d'analyser et d'ajuster ses comportements en ligne. À partir de situations proches de leurs usages quotidiens — profils, publications, traces, paramètres de confidentialité, données personnelles, temps d'écran — les élèves apprennent à identifier ce qui construit leur identité numérique et à mesurer les effets possibles de leurs actions sur eux-mêmes et sur les autres.

Le dispositif vise d'abord à faire comprendre que l'identité numérique n'est pas unique ni figée. Elle se construit à partir d'informations publiées volontairement, mais aussi de traces générées parfois sans intention directe : historiques, cookies, géolocalisation, likes, commentaires, partages, identifiants ou métadonnées. Les élèves sont donc amenés à distinguer les traces volontaires et involontaires, à comprendre leur permanence relative et à prendre conscience que les frontières entre espaces privé, public, familial, amical ou scolaire peuvent rapidement se brouiller.

La séquence conduit ensuite les élèves à repérer les données personnelles qu'ils communiquent dans les environnements numériques et à comprendre les risques associés : exposition excessive, perte de contrôle, usurpation, ciblage, cyberharcèlement, cybermanipulation ou atteinte à la vie privée. Elle les amène également à identifier des leviers d'action : paramétrer la confidentialité d'un compte, limiter la diffusion d'informations, effacer des traces de connexion sur un équipement partagé, signaler ou bloquer un contenu inapproprié, demander de l'aide et mobiliser des droits numériques simples comme le droit à l'oubli ou le droit de retrait.

Le dispositif travaille aussi la dimension d'équilibre de vie. Les élèves analysent leurs habitudes numériques et questionnent l'impact des plateformes sur leur attention, leur temps disponible, leurs relations et leur bien-être. Ils sont amenés à repérer leurs habitudes, à comprendre en quoi cette analyse peut améliorer leur organisation du temps et à identifier les bénéfices du droit à la déconnexion pour eux-mêmes et pour les autres.

À travers les cinq séances prévues, les élèves passent progressivement de la compréhension à l'action : ils comparent des profils selon différents contextes, analysent et classent des traces numériques,

observent la propagation d'une information, réalisent un audit de données personnelles, puis formulent un engagement personnel de citoyenneté numérique.

a. Tableaux des contenus / attendus

Contenu / Savoirs	Attendu
Identité numérique, traces et données personnelles	Expliquer ce qu'est l'identité numérique.
Identité numérique, traces et données personnelles	Expliquer qu'il existe des collectes de données actives : profils, formulaires, messages, tags... et passives : métadonnées, cookies, géolocalisation...
Identité numérique, traces et données personnelles	Expliquer le lien entre identité numérique, traces et données personnelles.
Notions spécifiques liées à l'éthique des médias numériques	Utiliser, adéquatement en contexte, les notions et les termes dont droit à la vie privée, droit à l'oubli, droit de retrait, liberté d'expression, censure, modération, licence open source, droit d'auteur.
Moyens d'agir face à un contenu inapproprié	Identifier les moyens de signaler ou bloquer un contenu partagé de manière inappropriée en ligne.
Risques numériques pour la personne	Expliquer les risques liés à l'exposition de données personnelles ou de contenus sensibles.
Culture numérique	Expliquer les principaux enjeux de l'utilisation des médias numériques sur le bien-être physique, psychologique et social.

Contenu / Savoir-faire	Attendu
Repérer les informations relatives à la vie privée, lors de l'encodage de données personnelles	Repérer les informations relatives à la vie privée, lors de l'encodage de données personnelles, y compris avec une IA.
Préserver la confidentialité ou l'anonymat	Préserver la confidentialité ou l'anonymat, lors de partage de contenus, y compris avec une IA.
Respecter les droits à l'image et à la voix	Respecter le droit à l'image et à la voix, dans des situations de communication et de collaboration.

Réagir face à des situations de cyberattaque, de cyberharcèlement, de cybermanipulation	Proposer et mettre en place des actions pertinentes pour faire face à des situations de cyberattaque, de cyberharcèlement, de cybermanipulation.
Respecter les droits de propriété	Respecter les droits de propriété, dans des situations de communication, y compris avec une IA.

Contenu / Compétences	Attendu
Gérer son identité numérique, ses traces et ses données personnelles, pour protéger sa vie privée et celle des autres	Gérer son identité numérique, ses traces, ses données personnelles, de manière responsable.
Prévenir et limiter les risques de déséquilibre social et psychologique de la personne	Réagir, de manière responsable, face aux risques de cyberattaque, de cyberharcèlement, de cyberdépendance.
Interagir / communiquer	Interagir et communiquer de manière orale et écrite, en sélectionnant et en utilisant des outils numériques adéquats.

b. Renvoi aux référentiels

Cette séquence s'inscrit prioritairement dans le volet numérique du référentiel FMTTN, dans les champs Sécurité, Communication et collaboration et, de manière complémentaire, Informations et données.

Elle cible plus particulièrement la gestion de l'identité numérique, des traces et des données personnelles, ainsi que la protection de sa vie privée et de celle des autres. Les élèves apprennent à identifier les informations qui participent à leur identité numérique, à distinguer les traces volontaires et involontaires et à adopter des gestes de protection adaptés.

La séquence mobilise également les apprentissages liés à l'éthique des médias numériques : droit à la vie privée, droit à l'oubli, droit de retrait, liberté d'expression, modération, droit à l'image, droit à la voix et respect d'autrui dans les environnements numériques.

L'intelligence artificielle peut être abordée de manière transversale lorsque les élèves questionnent la collecte de données, le profilage, la personnalisation des contenus ou l'usage d'outils qui traitent automatiquement des informations personnelles. L'objectif n'est pas de centrer la séquence sur l'IA, mais de faire comprendre que certaines données peuvent être exploitées par des systèmes automatisés et qu'il convient d'adopter une attitude prudente.

3. Lectures associées à cette séquence

a. Renvoi aux repères méthodologiques généraux

Cette séquence mobilise prioritairement les repères suivants : créer un climat de classe engageant, expliciter les démarches et les apprentissages, développer les autonomies, garder une trace des apprentissages, différencier pour soutenir les apprentissages et évaluer pour soutenir les apprentissages.

Ces repères soutiennent la prise de conscience progressive des élèves face à leurs pratiques numériques, dans un cadre bienveillant et non culpabilisant. Les activités proposées invitent les élèves à observer, questionner et ajuster leurs comportements sans exposer publiquement leur vie privée. Les traces écrites, l'audit personnel et le contrat de citoyenneté numérique permettent d'institutionnaliser les apprentissages et de favoriser leur transfert vers des situations concrètes de la vie quotidienne.

b. Renvoi aux repères méthodologiques disciplinaires

Dans le volet numérique de la FMTTN, cette séquence privilégie une approche active, réflexive et contextualisée. Les élèves observent des usages proches de leur quotidien, analysent des situations fictives ou anonymisées, identifient les risques liés aux traces et aux données personnelles, puis formulent des actions concrètes pour protéger leur vie privée.

La démarche articule compréhension, analyse et transfert : comprendre les notions d'identité numérique, de traces et de données personnelles ; consolider ces apprentissages par des classements, simulations et audits ; transférer les acquis dans un engagement personnel de citoyenneté numérique. Une attention particulière est portée à la confidentialité. Les situations sensibles sont traitées à partir de profils fictifs, de cas génériques ou de situations anonymisées. L'objectif est de développer la capacité d'action des élèves sans les placer dans une situation d'exposition ou de jugement.

4. Mise en contexte

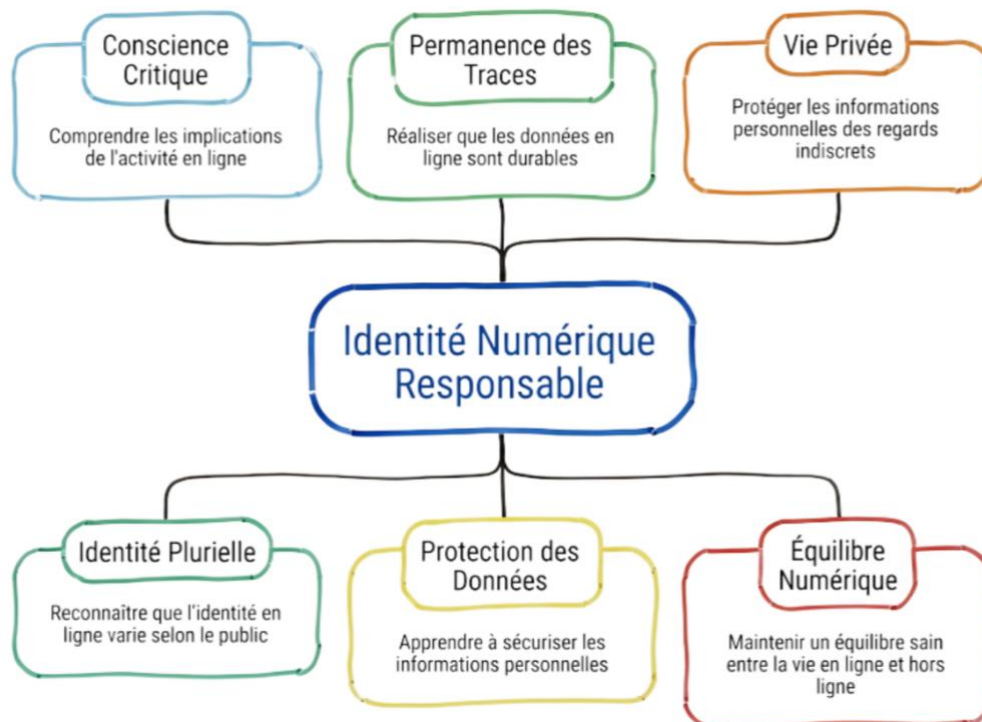
Les élèves de S1 utilisent régulièrement des environnements numériques : messageries, plateformes de vidéos, jeux en ligne, réseaux sociaux, outils scolaires, applications de communication ou espaces de stockage. Ils publient, likent, commentent, partagent, recherchent, s'inscrivent et acceptent parfois des conditions d'utilisation sans toujours mesurer les traces laissées ni les conséquences possibles.

Cette séquence vise à les rendre acteurs responsables de leur présence en ligne. Elle leur permet de comprendre que l'identité numérique est plurielle : l'image que l'on donne à des amis n'est pas nécessairement celle que l'on souhaite donner à sa famille, à l'école ou à des personnes inconnues. Elle amène aussi les élèves à comprendre que les traces numériques peuvent être durables, copiées, partagées ou exploitées dans d'autres contextes.

Un enjeu important concerne la confusion entre espace privé et espace public. Les élèves peuvent penser qu'un message envoyé à un petit groupe, une photo supprimée ou un compte réglé en mode privé ne présentent plus aucun risque. La séquence permet de nuancer ces représentations : un contenu peut être capturé, transféré, enregistré ou réutilisé.

La séquence aborde également l'équilibre de vie. Elle invite les élèves à questionner leurs habitudes numériques, leur temps d'écran, leur attention, leur sommeil, leurs relations et leur bien-être. L'objectif n'est pas de condamner les usages numériques, mais d'aider les élèves à identifier ce qui les aide, ce qui les influence et ce qu'ils peuvent ajuster.

Construire une Identité Numérique Responsable



Moment possible dans l'année

Cette séquence peut être menée après une première approche de la communication numérique, du droit à l'image ou de la recherche d'information. Elle peut également être proposée en début d'année afin d'installer des règles communes de communication, de confidentialité et de respect dans les environnements numériques utilisés en classe.

Elle peut être particulièrement pertinente avant un projet impliquant une publication, une production collaborative, un partage de fichiers ou l'usage d'un espace numérique de travail.

Prérequis possibles

Les élèves devraient idéalement avoir déjà rencontré quelques notions ou gestes simples :

- distinguer un profil, un compte et une publication ;
- comprendre qu'un contenu peut être partagé ou transféré ;
- identifier quelques données personnelles : nom, prénom, adresse, photo, localisation, identifiant ;
- connaître quelques règles de respect dans la communication ;
- comprendre qu'un mot de passe doit rester confidentiel ;
- utiliser un environnement numérique scolaire.

Ces prérequis peuvent varier fortement selon les élèves. Il est donc nécessaire de prévoir une vérification rapide des représentations et de s'appuyer sur des exemples simples, fictifs ou anonymisés.

Matériel nécessaire

- Ordinateurs, tablettes ou supports papier selon l'équipement disponible.
- Profils fictifs à comparer.
- Exemple de journée numérique fictive.
- Cartes ou supports de classement des traces numériques.
- Fiche « Qui peut voir ? ».
- Modèle d'audit de données personnelles.
- Compte fictif ou capture d'écran de paramètres de confidentialité.
- Fiche de vocabulaire.
- Support pour le contrat de citoyenneté numérique.
- Vidéoprojecteur ou écran pour les mises en commun.

Points de vigilance généraux

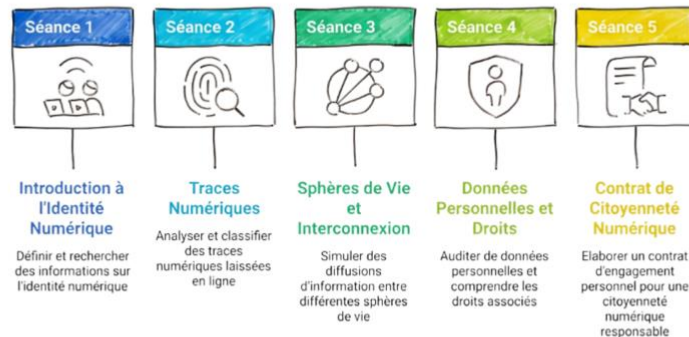
Les activités ne doivent pas conduire les élèves à révéler publiquement des informations personnelles. L'enseignant privilégie les profils fictifs, les cas anonymisés et les situations génériques. Il est important de ne pas culpabiliser les élèves. Certains usages numériques peuvent être maladroits, mais l'objectif est de construire une compréhension critique et des moyens d'action. Les formulations devront donc valoriser la progression : « Que puis-je faire pour mieux protéger mes données ? » plutôt que « Qu'ai-je fait de mal ? ».

Certaines discussions peuvent faire émerger des situations sensibles : cyberharcèlement, diffusion non consentie d'une image, pression sociale, mal-être, exposition excessive ou conflit entre élèves. Ces situations doivent être accueillies avec prudence, dans le respect du cadre de l'établissement et avec l'aide des personnes ressources si nécessaire.

5. Aperçu des étapes méthodologiques-clés de l'activité

Cette rubrique reprend de manière synthétique les étapes didactiques de la séquence. Elle ne détaille pas les modalités pratiques afin de permettre une prise en main rapide de l'activité.

Programme de Citoyenneté Numérique



Made with Napkin

Étape	Intention pédagogique	Ce que les élèves construisent
1. Comprendre l'identité numérique	Comprendre que l'identité numérique est plurielle et dépend des contextes.	Les élèves identifient les composantes d'une identité numérique et adaptent leur présentation selon les situations.
2. Identifier les traces numériques	Distinguer les traces volontaires et involontaires.	Les élèves repèrent les traces laissées en ligne et identifient des gestes pour les limiter.
3. Comprendre l'interconnexion des sphères de vie	Comprendre que les frontières entre privé, public, familial, amical et scolaire peuvent se brouiller.	Les élèves analysent la propagation d'un contenu et adaptent leurs comportements.
4. Protéger ses données personnelles	Identifier les données personnelles et connaître des droits numériques simples.	Les élèves réalisent un audit de données et repèrent des paramètres de confidentialité.
5. Construire un engagement citoyen	Réinvestir les apprentissages dans des gestes concrets.	Les élèves formulent un contrat personnel de citoyenneté numérique et d'équilibre de vie.

6. Intention de l'activité

a. Intention rédigée à destination des enseignants

L'intention de cette séquence est d'amener les élèves à comprendre ce qui construit leur identité numérique, à identifier les traces qu'ils laissent dans les environnements numériques, à repérer les informations relatives à leur vie privée et à adopter des comportements responsables pour protéger leurs données personnelles et celles des autres.

La séquence vise également à développer la capacité des élèves à réagir face à des situations à risque : exposition de données, partage non maîtrisé, atteinte à la vie privée, cyberharcèlement, cybermanipulation ou contenu inapproprié. Elle les amène à connaître des moyens d'action simples : paramétrer, limiter, supprimer, signaler, bloquer, demander de l'aide et exercer certains droits numériques.

Enfin, elle invite les élèves à questionner leurs habitudes numériques afin de favoriser un meilleur équilibre entre vie en ligne et vie hors ligne.

b. Annonce de l'objectif aux élèves

Nous allons apprendre à mieux comprendre notre identité numérique et les traces que nous laissons en ligne.

Pour y arriver, vous allez analyser des profils, repérer des traces numériques, comprendre comment une information peut circuler, identifier des données personnelles et construire des gestes concrets pour protéger votre vie privée, respecter celle des autres et garder un meilleur équilibre dans vos usages numériques.

7. Déroulement proposé de la séquence

Séance 1 – Qu'est-ce que l'identité numérique ?

Objectif de la séance

Amener les élèves à comprendre que l'identité numérique est plurielle et se construit différemment selon les contextes.

Activité principale

Les élèves comparent trois profils fictifs associés à différents contextes : amis, famille, école. Ils repèrent les différences de langage, d'images, de centres d'intérêt, d'informations partagées et de comportements.

Consignes aux élèves

- Observez les trois profils fictifs
- Repérez les informations visibles
- Comparez le langage utilisé
- Identifiez ce qui change selon le contexte

- Distinguez ce qui relève de la vie personnelle, de l'activité en ligne et de la réputation
- Choisissez les informations qui peuvent être partagées dans chaque contexte
- Justifiez vos choix

Trace d'apprentissage

Les élèves conservent :

- une définition collective de l'identité numérique ;
- une liste des composantes possibles : identité personnelle, identifiants, publications, activités, réputation ;
- une carte mentale simple de l'identité numérique, construite à partir d'un exemple fictif.

Point d'attention pour l'enseignant

Il est préférable de travailler à partir de profils fictifs afin d'éviter toute exposition d'élèves. L'enseignant veille à montrer que l'identité numérique peut varier selon les contextes, sans devenir fausse ou trompeuse : il s'agit d'adapter ce que l'on choisit de montrer.

Séance 2 – Traces numériques

Objectif de la séance

Amener les élèves à distinguer les traces volontaires et involontaires laissées lors des activités numériques.

Activité principale

Les élèves analysent une journée numérique fictive d'un adolescent. Ils identifient toutes les traces laissées au cours de la journée : messages, likes, commentaires, recherches, historique, cookies, géolocalisation, photos, métadonnées, connexions.

Consignes aux élèves

- Lisez la journée numérique fictive
- Soulignez les actions réalisées en ligne
- Identifiez les traces laissées volontairement
- Identifiez les traces laissées sans intention directe
- Classez les traces dans deux catégories : volontaires et involontaires
- Repérez les traces qui peuvent contenir des données personnelles
- Proposez trois gestes pour limiter certaines traces

Trace d'apprentissage

Les élèves conservent :

- un tableau de classement des traces volontaires et involontaires ;
- une courte définition de trace numérique ;
- trois gestes concrets pour limiter certaines traces : se déconnecter, limiter la géolocalisation, régler la confidentialité, effacer l'historique sur un appareil partagé, réfléchir avant de publier.

Point d'attention pour l'enseignant

Les élèves peuvent croire qu'une trace n'existe que lorsqu'ils publient volontairement quelque chose. Il est important de rendre visibles les traces moins évidentes, tout en évitant un discours anxiogène.

L'objectif est de comprendre pour mieux agir.

Séance 3 – Sphères de vie et interconnexion

Objectif de la séance

Amener les élèves à comprendre que les frontières entre vie privée et vie publique sont parfois floues dans les environnements numériques.

Activité principale

Les élèves participent à une simulation de propagation d'une information. Une publication fictive circule progressivement dans différents cercles : amis proches, groupe de classe, famille, école, public. Les élèves observent comment un contenu peut changer de destinataires et produire des effets non prévus.

Consignes aux élèves

- Observez la publication fictive
- Identifiez les premiers destinataires
- Suivez la circulation de l'information
- Repérez les nouveaux publics touchés
- Analysez les conséquences possibles du partage
- Complétez la fiche « Qui peut voir ? »
- Proposez des stratégies pour protéger la vie privée

Trace d'apprentissage

Les élèves conservent :

- une fiche « Qui peut voir ? » complétée ;
- une liste de risques liés à la diffusion : copie, capture d'écran, transfert, commentaire, sortie de contexte ;
- une liste de stratégies de protection : réfléchir avant de publier, demander l'accord d'une personne concernée, limiter l'audience, vérifier les paramètres, éviter les informations sensibles.

Point d'attention pour l'enseignant

L'enseignant veille à distinguer la situation fictive des expériences personnelles des élèves. La discussion doit porter sur les mécanismes de diffusion et non sur les comportements individuels de la classe.

Séance 4 – Données personnelles et droits numériques

Objectif de la séance

Amener les élèves à identifier les données personnelles qu'ils communiquent et à connaître quelques droits permettant de les protéger.

Activité principale

Les élèves analysent une inscription fictive à un réseau social, à une application ou à un service en ligne. Ils repèrent les informations demandées, distinguent les informations nécessaires et facultatives, puis découvrent quelques notions : données personnelles, consentement, droit à l'oubli, droit d'accès, droit de retrait, confidentialité.

Consignes aux élèves

- Observez le formulaire d'inscription fictif
- Repérez les informations demandées
- Entourez les données personnelles
- Distinguez les informations nécessaires et facultatives
- Identifiez les risques possibles en cas de diffusion
- Vérifiez les paramètres de confidentialité d'un compte fictif
- Proposez des réglages plus protecteurs

Trace d'apprentissage

Les élèves conservent :

- un audit simple de données personnelles ;
- une liste des données à protéger : nom, prénom, adresse, numéro, photo, localisation, identifiant, mot de passe, établissement scolaire ;
- une trace de vocabulaire : données personnelles, consentement, confidentialité, droit à l'oubli, droit d'accès, droit de retrait.

Point d'attention pour l'enseignant

L'enseignant évite de demander aux élèves de montrer leurs propres comptes ou paramètres personnels. L'activité doit s'appuyer sur un compte fictif, des captures préparées ou une simulation.

Séance 5 – Engagement citoyen et équilibre numérique

Objectif de la séance

Amener les élèves à mobiliser les acquis de la séquence dans un engagement personnel concret, réaliste et respectueux de leur équilibre de vie.

Activité principale

Les élèves analysent des situations numériques du quotidien : temps d'écran, notifications, partage de photos, mots de passe, confidentialité, publication dans un groupe, droit à la déconnexion. Ils formulent ensuite un contrat personnel de citoyenneté numérique comprenant trois engagements concrets.

Consignes aux élèves

- Lisez les situations proposées
- Identifiez le risque ou le problème
- Proposez une action responsable
- Choisissez trois engagements personnels
- Vérifiez que vos engagements sont réalistes
- Rédigez votre contrat de citoyenneté numérique
- Expliquez un engagement au groupe si vous le souhaitez

Trace d'apprentissage

Les élèves conservent :

- un contrat personnel de citoyenneté numérique ;
- trois engagements concrets et réalisables ;
- une courte réflexion sur l'équilibre numérique : temps d'écran, attention, sommeil, relations, droit à la déconnexion.

Point d'attention pour l'enseignant

Le contrat doit rester personnel et non intrusif. Les élèves ne doivent pas être forcés de révéler leurs habitudes numériques. Les engagements peuvent être formulés de manière générale : « Je vérifie avant de partager », « Je limite les informations personnelles », « Je respecte le droit à la déconnexion ».

8. Points de vigilance liés aux repères méthodologiques généraux

Créer un climat de classe engageant

La séquence aborde des thématiques directement liées à l'expérience personnelle des élèves. L'enseignant veille à instaurer un climat de confiance, respectueux et non jugeant. Les situations proposées doivent permettre la discussion sans exposer les élèves.

Expliciter les démarches et les apprentissages

Les notions doivent être rendues visibles et régulièrement reformulées : identité numérique, traces volontaires, traces involontaires, données personnelles, confidentialité, droit à l'oubli, droit de retrait, signalement, blocage, droit à la déconnexion. L'enseignant explicite également les démarches : observer, classer, analyser, mesurer un risque, choisir une action.

Différencier pour soutenir les apprentissages

Certains élèves peuvent recevoir des exemples déjà partiellement classés, une fiche de vocabulaire, des cartes de situations, une grille d'audit simplifiée ou des propositions d'engagements. Les élèves plus avancés peuvent analyser des situations plus complexes, comparer plusieurs paramètres de confidentialité ou rédiger une charte collective.

Développer les autonomies

L'autonomie se construit progressivement. Les élèves commencent par analyser des profils fictifs et des situations guidées, puis ils sont amenés à identifier eux-mêmes des gestes de protection et à formuler des engagements personnels.

Garder une trace des apprentissages

Les élèves conservent des traces variées : carte mentale, tableau de traces, fiche « Qui peut voir ? », audit de données personnelles, fiche de vocabulaire, contrat de citoyenneté numérique. Ces traces permettent de soutenir le transfert vers leurs usages réels.

Évaluer pour soutenir les apprentissages

L'évaluation accompagne la séquence et permet de réguler les apprentissages. Elle porte sur la compréhension des notions, la capacité à analyser une situation, à identifier un risque et à proposer une action responsable. Elle ne vise pas à juger les pratiques personnelles des élèves.

Protéger les élèves dans les échanges

Certaines activités peuvent faire émerger des situations de cyberharcèlement, de cybermanipulation, d'exposition non consentie ou de mal-être lié aux usages numériques. Ces situations doivent être accueillies avec prudence et bienveillance. Si nécessaire, l'enseignant oriente l'élève vers les personnes ressources de l'établissement.

9. Propositions de pratiques d'évaluation formative

L'évaluation formative accompagne l'ensemble de la séquence. Elle vise à soutenir les apprentissages et à observer la progression des élèves dans la compréhension de leur identité numérique, de leurs traces et des gestes de protection.

Elle permet d'observer :

- la capacité à expliquer ce qu'est l'identité numérique ;
- la capacité à distinguer traces volontaires et involontaires ;
- la capacité à identifier des données personnelles ;
- la compréhension du lien entre traces, données et identité numérique ;
- la capacité à reconnaître une situation à risque pour la vie privée ;
- la capacité à proposer une action de protection adaptée ;
- l'utilisation du vocabulaire spécifique ;
- la capacité à respecter le droit à l'image, à la voix et à la vie privée ;
- la capacité à formuler un engagement réaliste de citoyenneté numérique.

Modalités possibles

L'évaluation peut prendre plusieurs formes :

- observation des échanges en groupe ;
- vérification des tableaux de classement ;
- analyse de la fiche « Qui peut voir ? » ;
- retour oral sur les stratégies proposées ;
- vérification de l'audit de données personnelles ;
- autoévaluation individuelle ;
- contrat personnel de citoyenneté numérique ;
- retour collectif sur les gestes de protection.

Ces pratiques permettent à l'enseignant d'identifier les besoins des élèves pendant la séquence : difficulté à distinguer privé et public, à repérer une donnée personnelle, à comprendre la permanence des traces, à identifier un risque ou à choisir une action adaptée.

Le contrat de citoyenneté numérique réalisé en fin de parcours constitue une production de synthèse permettant d'observer la capacité des élèves à transférer les apprentissages vers des situations concrètes de leur vie quotidienne.

10. Liens avec les focus WBE

Citoyenneté numérique

La séquence contribue pleinement au développement d'une citoyenneté numérique éclairée, responsable et autonome. Les élèves apprennent à protéger leur vie privée, à respecter celle des autres, à gérer leurs traces et à adopter des comportements réfléchis dans les environnements numériques.

Éducation aux médias

Les élèves analysent les traces qu'ils produisent, comprennent que les plateformes peuvent collecter et exploiter des données personnelles et questionnent les mécanismes de personnalisation des contenus. Cette démarche favorise le développement de l'esprit critique face aux environnements numériques.

FLSco – Langue de scolarisation

La séquence permet de travailler un vocabulaire spécifique : identité numérique, trace, donnée personnelle, confidentialité, géolocalisation, cookie, métadonnée, droit à l'oubli, droit de retrait, e-réputation, signalement, blocage, cyberharcèlement, cybermanipulation. Les élèves sont amenés à utiliser ce vocabulaire pour expliquer leurs choix et justifier leurs stratégies.

Bien-être et santé

La séquence invite les élèves à analyser leurs habitudes numériques, leur temps d'écran, leur attention, leur sommeil, leurs relations et leur disponibilité. Elle permet d'aborder le droit à la déconnexion comme un moyen de préserver son équilibre et celui des autres.

Pensée critique et complexe

Les élèves apprennent à dépasser les évidences : un compte « privé » ne garantit pas un contrôle total, un message peut être transféré, une trace peut rester accessible, une donnée peut être exploitée dans un autre contexte. Ils développent ainsi une réflexion nuancée sur leurs usages numériques.

Prolongements possibles

La séquence peut être prolongée par la création d'une charte numérique de classe, d'une affiche de sensibilisation, d'une capsule vidéo ou d'un guide de bonnes pratiques destiné à d'autres élèves. Ces prolongements doivent rester centrés sur des conseils concrets, protecteurs et non culpabilisants.

11. Ressources digitales

Le Digipad associé aux séquences rassemble des ressources complémentaires destinées à soutenir leur mise en œuvre en classe : liens utiles, supports pédagogiques, exemples d'activités, outils numériques, vidéos, documents de référence et pistes d'approfondissement.

Il permet de centraliser les ressources dans un espace unique et facilement accessible

Son intérêt est aussi d'offrir un support évolutif. Dans le domaine du numérique, les outils, les usages, les plateformes, les ressources liées à l'IA ou à l'éducation aux médias évoluent rapidement. Le Digipad pourra donc être enrichi, adapté ou mis à jour au fil du temps, sans modifier l'ensemble des séquences.

Il constitue ainsi un espace d'appui pour les enseignants : chacun pourra y puiser des ressources en fonction de son matériel, de son groupe-classe, du temps disponible et des besoins observés chez les élèves.

