

 	<h2 style="margin: 0;">ÉVALUATION DE COMPÉTENCE</h2>	
NOM : Prénom :	Classe : Date :	

Observations et conseils de progrès

Référence aux compétences et connaissances évaluées

Thème abordé : OST – Les objets et les systèmes techniques : leurs usages et leurs interactions à découvrir et à analyser		
Attendu de fin de cycle : OST1 – Décrire les liens entre usages et évolutions technologiques des objets et des systèmes techniques		
Thématique : T2-Usages et impacts sociétaux du numérique		
Compétence OST15 – Identifier les règles permettant de sécuriser un environnement numérique (base de la cybersécurité) et les règles de respect de la propriété intellectuelle.	Connaissance OST1I-Cybersécurité : protection des données personnelles, traces numériques (témoins de connexion, géolocalisation), identification, authentification, respect de la propriété intellectuelle	Niveau atteint
Critères d'évaluation	N1 – Je sais que l'usage d'un environnement numérique nécessite des règles de sécurité,	
	N2 – et je sais que je dois sécuriser mes données et respecter les règles de propriété intellectuelle,	
	N3 – et je sais sécuriser mes données personnelles par des mots de passe forts,	
	N4 – et je sais effacer mes traces de navigation sur les navigateurs Internet	

N1 – Connaissance -

N1-1 Définir cyberviolence, usurpation d'identité, usage détourné

Relier le groupe de mots à la bonne définition :

La cyberviolence

Usage détourné

Usurpation d'identité

● ☐ Utilisation d'une image, d'une substance ou d'une information dans un but autre que celui pour lequel il a été conçu ou prévu.

● ☐ Actes malveillants commis par le biais des technologies numériques

● ☐ Utilisation de l'identité d'une personne sans son consentement pour commettre des actes malveillants

N2 – Compréhension

N2-1 – Identifier une situation de cyberviolence

Les situations proposées dans le tableau ci-dessous sont-elles de la cyberviolence ? Oui ou non ? Coche la bonne case.

Les situations proposées ci-dessous sont-elles de la cyberviolence ?	VRAI	FAUX
Diffuser des informations fausses ou trompeuses.		✗
Un individu crée un faux profil sur un réseau social en utilisant le nom et la photo d'une autre personne. Il se sert de ce faux profil pour diffuser de fausses informations et des messages blessants sur la victime	✗	
S'approprier le travail d'une autre personne		✗
Un désaccord ou une dispute en ligne qui ne dégénère pas en insultes ou en menaces.		✗
Un groupe d'élèves envoie des messages haineux et des menaces à une camarade de classe sur les réseaux sociaux. Ils diffusent également des photos d'elle modifiées de manière humiliante.	✗	
Le partage d'informations ou d'actualités qui peuvent être choquantes ou dérangeantes.		✗

N3 – Application

N3-1 – Expliquer un phénomène de cyberviolence

Qu'est-ce que la cyberviolence ? Quelles formes peuvent-elles prendre ?

Cyberviolence : Actes malveillants commis par le biais des technologies numériques, tels que les insultes, les menaces, le harcèlement ou la diffusion de photos ou vidéos privées.

Elle peut prendre la forme de **l'exclusion**, du **flaming**, de **l'usurpation d'identité**, du **outing** ou du **happy slapping**.

.....

N4 - Maîtrise

N4-1 – Mettre en place une procédure pour réagir contre des faits de cyberviolence

Que doit-on faire si nous sommes victimes ou témoins d'une situation de cyberviolence ?

- Ne pas répondre aux cyberviolences : ignorer les messages et les commentaires haineux.
- Conserver les preuves : sauvegarder les messages, les commentaires et les captures d'écran des cyberviolences.
- En parler à un adulte de confiance : parents, professeurs, éducateurs ou responsables associatifs.
- Signaler les cyberviolences : aux plateformes sur Internet et aux autorités
- Appeler le 3018