

Educational Technology & E-Learning Safety Guidelines

To ensure secure and effective use of educational technology and online learning platforms, follow these recommendations.

1. Privacy and Data Protection

- Collect only essential student information.
- Use platforms that comply with privacy laws like GDPR or COPPA.
- Store and transmit data in encrypted form.

2. Secure Access and Authentication

- Require strong, unique passwords for all accounts.
- Enable multi-factor authentication when possible.
- Immediately revoke access for inactive or unauthorized users.

3. Safe Communication

- Monitor discussion forums and chat rooms to prevent harassment.
- Encourage respectful online behavior.
- Provide reporting channels for inappropriate content.

4. Content Quality and Accuracy

- Verify the reliability of educational resources and tools.
- Regularly update materials to maintain accuracy.
- Use reputable sources for learning content.

5. Cybersecurity Practices

- Keep all software and learning management systems updated.
- Educate students and staff about phishing and malware risks.
- Back up digital content regularly.

6. Digital Well-Being

- Set reasonable screen time limits to reduce fatigue.
- Promote balanced schedules including offline activities.
- Encourage ergonomic setups for safe learning environments.

7. Parental and Institutional Oversight

- Inform parents or guardians about data use and platform policies.
- Provide training for teachers on secure e-learning practices.
- Conduct periodic security and privacy audits.

Applying these guidelines helps create safe, inclusive, and productive e-learning experiences.

1.

-

- GDPR COPPA

-

2.

-

-

-

3.

-

-

-

4.

-

-

-

5.

-

-

-

6.

-

-

-

7.

-

-

-

1.

-

-

-

2.

-

-

-

3.

-

-

-

4.

-

-

-

5.

-

-

-

6.

-

-

-

7.

-

-

-

Guía de Seguridad para Tecnología Educativa y Aprendizaje en Línea

Para garantizar un uso seguro y efectivo de la tecnología educativa y las plataformas de e-learning, siga estas recomendaciones.

1. Privacidad y Protección de Datos

- Recoja solo la información de los estudiantes que sea esencial.
- Use plataformas que cumplan con las leyes de privacidad como GDPR o COPPA.
- Almacene y transmita los datos de forma cifrada.

2. Acceso y Autenticación Seguros

- Exija contraseñas fuertes y únicas para todas las cuentas.
- Active la autenticación multifactor siempre que sea posible.
- Revoque de inmediato el acceso de usuarios inactivos o no autorizados.

3. Comunicación Segura

- Supervise foros de discusión y chats para prevenir el acoso.
- Fomente un comportamiento en línea respetuoso.
- Ofrezca canales para reportar contenido inapropiado.

4. Calidad y Precisión del Contenido

- Verifique la confiabilidad de los recursos educativos.
- Actualice los materiales con regularidad.
- Utilice fuentes reconocidas para los contenidos.

5. Prácticas de Ciberseguridad

- Mantenga todo el software y los sistemas de aprendizaje actualizados.
- Eduque a estudiantes y personal sobre riesgos de phishing y malware.
- Haga copias de seguridad de los contenidos digitales con frecuencia.

6. Bienestar Digital

- Establezca límites razonables de tiempo frente a la pantalla.
- Promueva actividades fuera de línea.
- Recomiende configuraciones ergonómicas para el estudio.

7. Supervisión de Padres e Instituciones

- Informe a padres o tutores sobre el uso de datos y las políticas de la plataforma.
- Capacite a los docentes en prácticas seguras de e-learning.
- Realice auditorías periódicas de seguridad y privacidad.

Con estas medidas se garantiza un aprendizaje en línea seguro, inclusivo y productivo.

Guide de Sécurité pour les Technologies Éducatives et l'Apprentissage en Ligne

Pour assurer une utilisation sûre et efficace des technologies éducatives et des plateformes d'e-learning, appliquez ces recommandations.

1. Confidentialité et Protection des Données

- Ne collectez que les informations essentielles des étudiants.
- Utilisez des plateformes conformes aux lois telles que le RGPD ou le COPPA.
- Stockez et transmettez les données sous forme chiffrée.

2. Accès Sécurisé et Authentification

- Exigez des mots de passe forts et uniques pour chaque compte.
- Activez l'authentification multifactor lorsque c'est possible.
- Révoquez immédiatement l'accès des utilisateurs inactifs ou non autorisés.

3. Communication Sécurisée

- Surveillez les forums de discussion et les chats pour éviter le harcèlement.
- Favorisez un comportement en ligne respectueux.
- Offrez des moyens de signaler tout contenu inapproprié.

4. Qualité et Exactitude du Contenu

- Vérifiez la fiabilité des ressources pédagogiques.
- Mettez régulièrement à jour les supports d'apprentissage.
- Utilisez des sources reconnues.

5. Cybersécurité

- Maintenez à jour tous les logiciels et systèmes de gestion de l'apprentissage.
- Sensibilisez élèves et enseignants aux risques de phishing et de malware.
- Sauvegardez régulièrement le contenu numérique.

6. Bien-être Numérique

- Fixez des limites raisonnables de temps d'écran.
- Encouragez les activités hors ligne.
- Assurez des postes de travail ergonomiques.

7. Supervision Parentale et Institutionnelle

- Informez les parents sur l'utilisation des données et les politiques de la plateforme.
- Formez les enseignants aux pratiques de e-learning sécurisées.
- Effectuez des audits réguliers de sécurité et de confidentialité.

Ces pratiques garantissent une expérience d'apprentissage en ligne sûre et inclusive.

1.

-

-

GDPR COPPA.

2.

-

-

3.

-

-

-

4.

-

-

-

5.

-

-

-

6.

-

-

-

7.

-

-

-