#TOPIC 6

SENSITISING ADULT LEARNERS FOR DATA PRIVACY AND SAFETY

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Sensitising adult learners for data privacy and safety

Topic	Sensitising adult learners for data privacy and safety
Description of the topic	Sensitising adult learners for data privacy and safety involves raising awareness about the importance of protecting personal information in digital environments. This process equips learners with the knowledge and skills to recognise potential risks and adopt safe practices. Through interactive training sessions and discussions of real-world scenarios, educators can empower adult learners to take proactive steps in safeguarding their data and understanding their rights under data protection regulations.
Title of tool	"Practical steps to tackle key challenges when it comes to navigating data protection legislation"
Link to the tool	https://cstuk.org.uk/news-publications/cst-blogs/tackling-data-protection-challenges-in-schools/
About the tool	The CST blog article highlights strategies for schools to tackle data protection challenges, closely aligning with adult education on data privacy. It addresses common issues, such as responding to Subject Access Requests (SARs), securely handling data, and mitigating cyber threats—key concerns in educational institutions. Schools are encouraged to train staff, securely store data, and implement cybersecurity practices, which serve as practical examples for data privacy sensitisation among adult learners. These insights support building robust privacy awareness within educational settings.

Topic	Sensitising adult learners for data privacy and safety
Description of the topic	This topic addresses the growing importance of understanding and applying data privacy and safety principles. It aims to educate adult learners on protecting personal and sensitive information in online environments, ensuring compliance with data protection regulations like GDPR, and fostering a secure digital presence.
Title of tool	"Data protection and privacy training"
Link to the tool	https://www.youtube.com/watch?v=aZdsiLTdaT0

About the tool	The video titled "Data Protection and Privacy Training - Lesson 1" is an educational resource designed to explain the complexities of data protection and privacy policies. Created by the Synthesia team, it aims to simplify and clarify these sometimes challenging topics.

Topic	**Sensitising adult learners for data privacy and safety**
Description of the topic	This topic focuses on educating adult learners about the importance of online safety and data privacy. It aims to equip them with the knowledge and skills necessary to navigate the internet securely, protecting their personal information from potential threats.
Title of tool	"Being Safe on the Internet"
Link to the tool	https://www.youtube.com/watch?v=HxySrSbSY7o
About the tool	This video provides practical tips for maintaining safety while exploring the internet. It emphasises the importance of being cautious about the information shared online and offers guidance on how to protect oneself from potential online risks. The objective is to raise awareness about online safety practices and encourage responsible internet usage.

Section	Description
Module Title	Building Awareness of Data Privacy and Safety in Online Learning
Overview of the topic	This module introduces the fundamental principles of data privacy and safety in online environments, helping educators protect their own data and guide learners to do the same.
Objective	1. Educators will understand the basic principles of data privacy and safety in online teaching. 2. Learners will be equipped to recognise and mitigate risks to their personal data in digital environments. 3. Both educators and learners will be empowered to adopt best practices for protecting sensitive information online.
Relevant Regulations/Standards	- **General Data Protection Regulation (GDPR):** Explains how personal data should be collected, stored, and processed safely - **ePrivacy Directive:** Outlines rules for online privacy and data protection in electronic communications
Implications for Adult Education	Data privacy and safety are critical for adult learners, who often use personal devices and accounts for online learning. Educators must ensure secure practices to build trust and provide a safe learning environment. Integrating these topics raises awareness and protects against real-world cyber threats.
Activities/Exercises	1. *Role-Playing*: Divide learners into groups to simulate common privacy risks (e.g., phishing emails or oversharing on social media) and discuss solutions. 2. *Data Audit*: Learners list the personal information they share online and discuss how to reduce their digital footprint.
Methodological Guidance	1. Begin the session with a relatable story or case study to illustrate the importance of data privacy. 2. Use simple language to explain concepts and avoid technical jargon.

	3. Encourage learners to share their own experiences with data privacy challenges to make the discussion interactive.
Explanatory Notes	Phishing: A fraudulent attempt to obtain sensitive information by pretending to be a trustworthy entity. Digital Footprint: The trail of data users leave behind while using digital devices or services.
Definitions and Key Terms	- GDPR: A legal framework setting guidelines for the collection and processing of personal data. - Data Breach: An incident where sensitive data is accessed or disclosed without authorisation. - Encryption: The process of converting information into a secure format to prevent unauthorised access.
Examples/Case Studies	*Case Study*: A teacher used an unsecured online platform for a class, and a malicious actor accessed the session and disrupted the learning environment. This example highlights the importance of using secure tools and setting passwords.

(a) Implementing Tools

Topic	Sensitising adult learners for data privacy and safety
Description of the topic	Sensitising adult learners for data privacy and safety involves raising awareness about the importance of protecting personal information in digital environments. This process equips learners with the knowledge and skills to recognise potential risks and adopt safe practices. Through interactive training sessions and discussions of real-world scenarios, educators can empower adult learners to take proactive steps in safeguarding their data and understanding their rights under data protection regulations.
Title of tool	"Minding the data: protecting learners' privacy and security"
Link to the tool	https://www.right-to-education.org/resource/minding-data-protecting-learners-privacy-and-security
About the tool	The UNESCO report "Minding the Data: Protecting Learners' Privacy and Security" examines the balance between using educational data for improvement and safeguarding student privacy. It highlights the risks of data misuse, calls for robust privacy policies, and promotes collaboration in international policy development. This resource is particularly relevant for raising awareness among educators and learners about data privacy within digital education environments.

CHECKLIST

Secure online teaching session step-by-step	
☐	Verify that the digital platform used complies with GDPR by reviewing the platform's privacy policy for data handling practices
☐	Set up password protection or access restrictions to teaching material for secure access
☐	Ensure documented consent of students if you want to take photos of the teaching session
☐	Choose secure communication channels for sharing the details of the session
Notes: Adult educators can use this checklist for ensuring a secure online teaching session. It supports educators in systematically addressing data privacy and protection needs throughout the pre-session phase.	

CHECKLIST

Preparation for a Safe Online Teaching Session	
☐	Select a trusted platform (e.g., Zoom, Microsoft Teams) and familiarise yourself with its basic settings
☐	Ensure your internet connection is secure and avoid using public Wi-Fi
☐	Update your device with the latest security patches and install antivirus software
☐	Set up a password-protected meeting link to restrict access to authorised participants
☐	Plan to collect only the minimum necessary information from participants (e.g., first name or alias)
☐	Prepare teaching materials in advance and save them in a secure location
Notes: If unsure how to set up secure links or update devices, ask for help from a colleague or a tech support team.	

CHECKLIST

Maintaining Privacy and Safety While Teaching Online

☐	Admit only authorised participants to the session (e.g., through a waiting room feature)
☐	Avoid sharing participant names, emails, or personal details during the session
☐	Use secure methods to share materials (e.g., file-sharing tools provided by the platform)
☐	Remind participants of basic privacy rules, such as not sharing the meeting link or recording the session without permission
☐	Monitor the chat and screen-sharing features to ensure no unauthorised content is shared

Notes: Pause to address privacy or safety concerns if they arise during the session.

CHECKLIST

Post-Session Privacy and Follow-Up

☐	Do not store or share unnecessary participant data (e.g., names or attendance lists)
☐	Ensure that session recordings, if made, are stored securely and shared only with authorised participants
☐	Share any follow-up materials or resources using secure platforms (e.g., email or private links)
☐	Encourage participants to review tips on protecting their data and provide relevant resources
☐	Evaluate the session and note any privacy or safety issues to improve future sessions

Notes: Take a moment to review GDPR basics if you're unsure about data storage or sharing.

GUIDE: Teaching Data Privacy and Safety in Online Sessions

A Practical Guide for Adult Educators to Promote Privacy Awareness

Objective: To help adult educators introduce the importance of data privacy and safety to learners during online teaching sessions, ensuring a secure and aware learning environment.

Scenario: An adult educator is preparing to conduct an online session for a group of learners unfamiliar with basic data privacy principles. During registration, learners are asked to share their email addresses, and during the session, they might accidentally reveal personal information in the chat. The educator must ensure privacy is protected and learners understand how to stay safe online.

Guidance:

Before the Session:

1. Choose Secure Platforms: Use trusted tools like Zoom or Microsoft Teams. Ensure they are updated and configured with GDPR-compliant settings.
2. Minimise Data Collection: Only ask for essential information during registration (e.g., first name, email). Avoid collecting unnecessary personal details.
3. Prepare Privacy Rules: Prepare and share simple privacy ground rules for the session, such as "Do not share sensitive information in the chat." Share these with participants beforehand.
4. Test the Platform: Familiarise yourself with features like muting participants, locking meetings, and enabling waiting rooms.

During the Session:

1. Start with Awareness: Begin the session by briefly explaining why data privacy matters and providing examples of common risks (e.g., phishing emails, unsecured websites).
2. Model Safe Practices: Avoid calling out full names or sharing personal information about participants. Refer to them by first name or aliases.
3. Engage Safely: Use interactive tools like polls or Q&A features to engage learners without requiring them to disclose personal information.
4. Monitor the Chat: Watch for and address any accidental sharing of sensitive details in the chat. Remind participants of privacy rules when needed.

After the Session:

1. Secure Materials: Save recordings, if any, in a password-protected folder and only share them with authorised individuals.
2. Provide Resources: Share a simple guide or checklist on staying safe online, tailored to the session's content.
3. Reflect and Improve: Note any privacy challenges during the session and adjust your approach for next time.

Practical tips:
Use relatable examples, such as "Think of your personal data like your house keys—don't give them to just anyone!" to help learners understand the importance of protecting their information.