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.