#TOPIC 7

STORAGE AND PROCESSING OF LEARNER DATA

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.

Storage and processing of learner data

Tool 1:

Topic	**Storage and processing of learner data**
Description of the topic	The secure storage and responsible processing of learner data are critical components of data protection. Storage involves utilising encrypted databases, secure cloud solutions, and regular audits to ensure the integrity and confidentiality of the data. Processing focuses on handling learner information in compliance with GDPR requirements, employing techniques like anonymisation where appropriate, and adhering to clear retention and deletion policies. These practices ensure that learner data is both securely stored and ethically managed throughout its lifecycle.
Title of tool	Secure Email Services
Link to the tool	• ProtonMail • Tutanota
About the tool	Secure email services like ProtonMail and Tutanota protect email communication with strong encryption, ensuring that sensitive information exchanged via email remains confidential. These services often include end-to-end encryption and secure servers to safeguard communications. This level of security is crucial for educational institutions where sensitive data is frequently shared. By using these services, educators can maintain the privacy and integrity of email communications.

Tool 2:

Topic	Storage and processing of learner data
Description of the topic	The secure storage and responsible processing of learner data are critical components of data protection. Storage involves utilising encrypted databases, secure cloud solutions, and regular audits to ensure the integrity and confidentiality of the data. Processing focuses on handling learner information in compliance with GDPR requirements, employing techniques like anonymisation where appropriate, and adhering to clear retention and deletion policies. These practices ensure that learner data is both securely stored and ethically managed throughout its lifecycle.
Title of tool	Secure File Sharing Platforms
Link to the tool	● Tresorit ● Sync ● Google Workspace
About the tool	Secure file sharing platforms like Tresorit, Sync, and Google Workspace (with proper access controls) safely distribute learning materials containing sensitive information. These platforms offer encryption and secure access controls, ensuring that only authorised users can access shared files. By using these platforms, educators can protect sensitive data while collaborating with colleagues or sharing resources with learners. This enhances data security and maintains compliance with data protection regulations.

Tool 3:

Topic	**Storage and processing of learner data**
Description of the topic	The secure storage and responsible processing of learner data are critical components of data protection. Storage involves utilising encrypted databases, secure cloud solutions, and regular audits to ensure the integrity and confidentiality of the data. Processing focuses on handling learner information in compliance with GDPR requirements, employing techniques like anonymisation where appropriate, and adhering to clear retention and deletion policies. These practices ensure that learner data is both securely stored and ethically managed throughout its lifecycle.
Title of tool	Learning Management Systems (LMS) with Security Features
Link to the tool	● Moodle ● Canvas
About the tool	Learning Management Systems (LMS) like Moodle and Canvas offer robust security features such as role-based access controls, activity logging, and encryption for all stored data. These features ensure that only authorised users can access sensitive information, maintaining data integrity and confidentiality within the LMS. By using these systems, educators can securely manage learning materials and track learner activities while protecting sensitive data. This helps maintain a secure learning environment.

Tool 4:

Topic	Storage and processing of learner data
Description of the topic	The secure storage and responsible processing of learner data are critical components of data protection. Storage involves utilising encrypted databases, secure cloud solutions, and regular audits to ensure the integrity and confidentiality of the data. Processing focuses on handling learner information in compliance with GDPR requirements, employing techniques like anonymisation where appropriate, and adhering to clear retention and deletion policies. These practices ensure that learner data is both securely stored and ethically managed throughout its lifecycle.
Title of tool	SFTP for Secure File Transfers
Link to the tool	• FileZilla • WinSCP
About the tool	Secure File Transfer Protocol (SFTP) tools like FileZilla and WinSCP ensure secure file transfers when sharing or submitting assignments. SFTP encrypts data during transfer, reducing the risk of data interception or unauthorised access. By using these tools, educators can securely exchange files with learners or colleagues, maintaining the confidentiality and integrity of sensitive information. This is essential for protecting learner data during file transfers.

Tool 5:

Topic	**Storage and processing of learner data**
Description of the topic	The secure storage and responsible processing of learner data are critical components of data protection. Storage involves utilising encrypted databases, secure cloud solutions, and regular audits to ensure the integrity and confidentiality of the data. Processing focuses on handling learner information in compliance with GDPR requirements, employing techniques like anonymisation where appropriate, and adhering to clear retention and deletion policies. These practices ensure that learner data is both securely stored and ethically managed throughout its lifecycle.
Title of tool	Data Retention and Deletion Tools
Link to the tool	• BleachBit • Eraser
About the tool	Data retention and deletion tools like BleachBit and Eraser securely delete learner data after it is no longer needed, ensuring compliance with data retention policies. These tools overwrite data multiple times, making it unrecoverable and reducing the risk of unauthorized access. By using these tools, educational institutions can maintain data security and adhere to legal requirements for data disposal. This helps prevent potential data breaches and maintain compliance.

Tool 6:

Topic	Storage and processing of learner data
Description of the topic	The secure storage and responsible processing of learner data are critical components of data protection. Storage involves utilising encrypted databases, secure cloud solutions, and regular audits to ensure the integrity and confidentiality of the data. Processing focuses on handling learner information in compliance with GDPR requirements, employing techniques like anonymisation where appropriate, and adhering to clear retention and deletion policies. These practices ensure that learner data is both securely stored and ethically managed throughout its lifecycle.
Title of tool	Backup and Recovery Tools
Link to the tool	• Acronis • Veeam
About the tool	Regular backup and recovery plans using tools like Acronis and Veeam ensure that learner data is securely backed up and can be restored in case of data loss or system failure. These tools provide robust backup solutions that maintain data integrity and availability, ensuring institutional continuity. By implementing these plans, educators can protect critical data and quickly recover from potential disruptions. This helps maintain the stability of educational operations.