THE DATA GAME Toolbox

Co-funded by the European Union

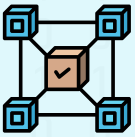
Funded by the European Union. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or OeAD-GmbH. Neither the European Union nor the granting authority can be held responsible for them. Project number: 2023-1-AT01-KA220-ADU-000157050

TOOL SECTIONS

ADMIN & TECHNOLOGY

LEGAL REQUIREMENTS & RESPONSIBILITY

TALKING PRIVACY & SAFETY



ACCESS, REGISTRATION, ADMINISTRATION

SECURITY IN EDUCATION TECHNOLOGIES

STORAGE & PROCESSING

DATA HANDLING & SECURITY

TRAINING & AWARENESS PROGRAMS

SOCIAL MEDIA APPS

TOOLS

ADMIN & TECHNOLOGY

1. DPIA TEMPLATES

Data Protection Impact Assessments (DPIAs) are essential tools used to assess potential risks to learner data before starting a course or project. They help organizations identify and mitigate risks associated with data processing, ensuring compliance with regulations like the General Data Protection Regulation (GDPR). DPIAs are particularly important in educational settings where sensitive personal data is often processed. By conducting a DPIA, educators can better understand the data protection risks involved in their projects, calculate methods to decrease or eliminate those risks, and document data protection measures to demonstrate compliance to supervisory authorities.

- GDPR EU
- IUBENDA
- TECHTARGET
- S.E.T.U.

2. PASSWORD MANAGEMENT

Password management tools like LastPass, 1Password, and Bitwarden ensure strong, unique passwords for access to educational systems and databases, reducing the risk of unauthorized access. These tools offer features like password vaults and auto-fill capabilities, making it easier to manage multiple secure passwords. By using these tools, educators can maintain robust security while simplifying their login processes. This helps prevent common security issues related to weak or reused passwords.

- LASTPASS
- 1PASSWORD
- BITWARDEN

TOOLS

ADMIN & TECHNOLOGY

3. E-PLATFORMS

Staff training modules on GDPR and data handling, available on platforms like Coursera and Udemy, are essential for ensuring that educators understand and comply with data protection regulations. These modules provide interactive learning experiences that help staff develop the skills needed to handle learner data securely. By using platforms like TalentLMS or Articulate 360, institutions can create tailored training programs to meet their specific needs. This training is vital for maintaining a culture of data security within educational settings.

- COURSERA
- UDEMY
- TALENTLMS
- ARTICULATE 360

4. PROTECTION & SECURITY

Cybersecurity frameworks like the CIS Controls Implementation Guide and the NIST Cybersecurity Framework provide guidelines for securing institutional systems and data. These frameworks outline best practices for cybersecurity, helping institutions implement robust security measures to protect against cyber threats. By following these frameworks, educational institutions can ensure that their data and systems are well-protected and compliant with industry standards. This proactive approach helps prevent data breaches and maintain institutional security.

- CIS CONTROLS
- NIST FRAMEWORK

TOOLS

ADMIN & TECHNOLOGY

5. VPN

Virtual Private Network (VPN) tools like NordVPN and ExpressVPN secure internet connections during virtual teaching sessions, especially on public networks. By encrypting data in transit, VPNs protect against eavesdropping and man-in-the-middle attacks, ensuring that sensitive information remains confidential. This is particularly important for educators who often work remotely or use public networks. Using VPNs helps maintain the security of educational communications.

- NORDVPN
- EXPRESS VPN

6. COMMUNICATION

- SIGNAL
- MS TEAMS

Privacy-focused communication tools like Signal and Microsoft Teams (with advanced security settings) encrypt video and text communication with learners. These tools provide end-to-end encryption and secure authentication mechanisms, ensuring that sensitive information exchanged during sessions remains confidential. By using these tools, educators can maintain the privacy of communications while collaborating with learners or colleagues. This enhances trust and compliance with data protection regulations.

7. AUDIT& MONITORING

Audit and monitoring software like Splunk and SolarWinds monitor data access and identify potential breaches post-session. These tools analyze logs and network activity to detect security incidents early, allowing institutions to take prompt action to mitigate damage.

By using these tools, educators can ensure that data security measures are effective and compliant with regulatory standards. This proactive monitoring helps maintain the integrity of educational systems.

TOOLS

ADMIN & TECHNOLOGY

8. BREACH NOTIFICATION

- SPLUNK
- SOLARWINDS
- GDPR ADVISOR

Privacy-focused communication tools like Signal and Microsoft Teams (with advanced security settings) encrypt video and text communication with learners. These tools provide end-to-end encryption and secure authentication mechanisms, ensuring that sensitive information exchanged during sessions remains confidential. By using these tools, educators can maintain the privacy of communications while collaborating with learners or colleagues. This enhances trust and compliance with data protection regulations.

9. ANNONYMOUS FEEDBACK TOOLS

Feedback mechanisms like Google Forms with encryption or Mentimeter allow educators to gather learner feedback on data security practices during courses. These tools provide secure platforms for anonymous feedback, helping educators identify areas for improvement in their data handling processes. By using these mechanisms, institutions can refine their data security practices and enhance learner trust. This feedback loop is essential for maintaining a secure and responsive educational environment.

- GOOGLE FORMS
- MENTIMETER
- FORMS APP

TOOLS

LEGAL REQUIREMENTS & RESPONSIBILITY

ACTIVITY 1

Present a scenario in which a teacher needs to decide whether to share student data with a third party.

- Discuss how GDPR compliance should influence the decision.
- Quiz: Include a quiz to test knowledge of GDPR principles.

Methodological Guidance

- Encourage educators to use real-life scenarios to discuss GDPR with their learners.
- Suggest including GDPR awareness as part of the orientation for students, particularly in courses involving online learning.
- Define key terms such as *personal data*, *consent*, and *data processing*.
- Provide case studies or examples of GDPR compliance breaches and their consequences in educational settings.

Definitions and Key Terms

- **GDPR (General Data Protection Regulation)**: The GDPR is a European Union regulation that sets rules for how personal data is collected, stored, and processed, aiming to enhance privacy protections.
- **Personal Data**: Any information that can directly or indirectly identify a person, such as name, email address, or IP address.
- **Data Controller**: An entity (e.g., an educational institution) that determines the purpose and means of processing personal data.
- **Data Processor**: A person or entity that processes data on behalf of the Data Controller (e.g., a cloud storage provider).
- **Consent**: Explicit permission given by individuals to process their data for specific purposes, which must be freely given, informed, and unambiguous.

Examples/Case Studies

- **Case Study 1**: An online teaching platform suffered a data breach, exposing learners' personal information, including email addresses

LEGAL REQUIREMENTS & RESPONSIBILITY

and passwords. The breach occurred because theplatform did not update its security protocols. As a result, the organisation faced heavy fines for non-compliance with GDPR and lost user trust.

- *Lesson*: Regularly update security systems and audit platforms used for data processing.

Case Study 2: An educator recorded an online session and shared it publicly on a complaint, citing unauthorised data usage. The institution was required to remove the recording and provide formal apologies.
Lesson: Always obtain consent for recording sessions and clarify where the recordings will be used.

Case Study 3: A school implemented a new digital attendance system without informing parents. Parents raised concerns about how their children's data was being processed and stored. Following the complaints, the school conducted a data privacy audit and introduced better communication policies about data collection.
Lesson: Transparency is critical—communicate the purpose and methods of data collection to all stakeholders.

ACTIVITY 2

Step-by-Step Advice for GDPR Compliance in Online and Classroom Teaching

An adult educator conducts online sessions using a popular video conferencing platform. During a session, the educator records the meeting to share with absent students. The educator also uses a shared online folder to distribute course materials. However, learners express concerns about how their personal data (e.g., video recordings, email addresses, and shared folder access logs) is being stored and whether it could be shared without their consent.

Step 1
Verify GDPR Compliance of Digital Tools:

- Before choosing a video conferencing platform, review its privacy policy to ensure

LEGAL REQUIREMENTS & RESPONSIBILITY

compliance with GDPR regulations. For example, check if the platform encrypts data and stores it in GDPR-compliant servers.
- If using a new tool, ensure your institution has signed a Data Processing Agreement (DPA) with the provider.

Step 2
Obtain Explicit Consent for Data Processing:

- Before recording sessions or collecting personal data, inform students about why their data is needed and how it will be used.
- Example: Use a consent form or include a clear notice at the start of each session stating the purpose of recording.

Step 3
Secure Communication Channels:

- Use password-protected links for sharing materials or conducting sessions.
- Example: Instead of sharing open-access links, require students to log in with their credentials to access shared resources.

Step 4
Limit Data Collection to What Is Necessary:

- Only collect data that is essential for the course. For instance, do not request personal details like home addresses unless absolutely necessary.

Step 5
Educate Learners on Their Privacy Rights:

- Include a short module or discussion about students' rights under GDPR, such as accessing, correcting, or deleting their personal data.
- Example: Share a document summarising their rights at the beginning of the course.

Step 6
Regularly Audit and Delete Unnecessary Data:

- Review data storage practices periodically. For example, delete old session recordings and access logs that are no longer required for educational purposes.

TOOLS

LEGAL REQUIREMENTS & RESPONSIBILITY

ACTIVITY 3

GDPR-related challenges and safeguarding for learner privacy

An institution launches an online course and requires learners to fill out a registration form with personal details, including phone numbers and demographic data. A learner requests their data to be removed after completing the course, raising questions about how the institution manages and deletes learner data.

Six Critical Steps for GDPR Compliance in Online and Classroom Teaching

Step 1
Legal Compliance:
- Ensure all data collection processes meet GDPR requirements by maintaining transparency. For example, use a privacy notice that clearly states why data is collected and how it will be used.

Step 2
Data Security:
- Store all personal data securely, using encrypted storage systems and limiting access to authorised personnel only.

Step 3
Consent Management:
- Before processing learner data, obtain explicit consent, such as for session recordings. Consent forms should be stored securely for future reference.

Step 4
Data Retention Policies:
- Define how long data will be stored and ensure unnecessary data is deleted after its purpose is served.

Step 5
Handling Data Requests:
- Respond promptly to learners who request access to, correction of, or deletion of their data.

Step 6
Institutional Training:

TOOLS

LEGAL REQUIREMENTS & RESPONSIBILITY

- Educate all staff involved in course delivery about GDPR compliance. Example: Conduct a workshop for educators on secure data management practices.

MAIN GDPR IMPLICATIONS FOR ONLINE AND CLASSROOM TEACHING

NEWS UPDATE

This UNESCO report highlights the balance between leveraging educational data and protecting learner privacy. It addresses key GDPR compliance challenges, such as managing consent, responding to data access requests, and implementing secure data handling practices. The tool offers actionable guidance for educators to safeguard learner data while ensuring compliance with privacy regulations, making it an invaluable resource for promoting safe and ethical data practices in education.

ASSESSMENT

The Data Protection Self-Assessment Toolkit, provided by the UK Information Commissioner's Office (ICO), is a practical tool designed to help organisations evaluate their compliance with data protection laws, including GDPR. This tool guides educators through various compliance aspects, such as data security, lawful processing, and rights management. It is especially useful for identifying gaps in current practices and implementing improvements, enabling educators to confidently manage data privacy in both online and classroom environments.

CHECKLIST FOR ONLINE TEACHING

Pre-session

Verify that any digital platforms used (e.g., video

TOOLS

LEGAL REQUIREMENTS & RESPONSIBILITY

conferencing tools, online assessments) comply with GDPR by reviewing their privacy policy and data protection practices.

Obtain explicit consent from students for collecting and processing their personal data (e.g., for online registrations, assessment data, etc.).

Secure access to teaching materials by password-protecting files or using secure platforms for sharing resources.

Inform students about their data protection rights, including their right to access and erase their data, and how their data will be used during the course.

During session

Use secure communication tools (e.g., encrypted email, password-protected online forums) for sharing sensitive information.

Ensure that student interactions, recordings, and chat logs are kept confidential and are only accessible to relevant parties.

Avoid collecting unnecessary personal data; only request what is required for the session.

Post-session

Delete or securely store session recordings, ensuring that access is restricted to authorised personnel only.

Update records and ensure proper documentation of student consent.

Regularly audit and review data handling practices to ensure ongoing GDPR compliance.

TOOLS

TALKING PRIVACY & SAFETY

Effective communication and transparency about data privacy and safety are essential in fostering trust and compliance in educational settings. As personal data becomes increasingly intertwined with digital learning, educators and institutions must ensure learners are informed about how their data is collected, processed, and protected. Transparent communication helps learners understand their rights under data protection laws like the General Data Protection Regulation (GDPR) and builds confidence in the institution's commitment to privacy.

Here are some strategies for effectively communicating data privacy and safety issues to learners

ACTIVITY 1

Communication and Transparency: Communicating Data Privacy and Safety Issues

- **GDPR Article 12**: Transparent information, communication and modalities for the exercise of the rights of the data subject
- **GDPR Article 13**: Information to be provided where personal data are collected from the data subject
- **GDPR Article 32**: Security of processing

Scenario Discussion

Present a situation where a learner expresses concern about the data collected during an online course. Discuss how educators should address these concerns transparently while maintaining compliance with GDPR.

Role-Play Activity

Educators practice explaining data privacy concepts to learners, such as consent and data retention, using simple and clear language.

Reflection Exercise

Ask educators to audit their current communication

TOOLS

TALKING PRIVACY & SAFETY

practices regarding data privacy and identify areas for improvement.

Methodological Guidance

- Use **accessible language** when discussing data privacy issues to ensure understanding among all learners. Transparency is key in building trust and ensuring compliance with privacy and protection laws.
- Share **practical examples** of data privacy practices within the course structure, such as how attendance records are maintained securely.
- Incorporate data **privacy discussions** into the curriculum to make learners active participants in protecting their information.

Definitions and Key Terms

- **Transparency**: The practice of openly sharing information about how personal data is collected, stored, and used.
- **Privacy Policy**: A document outlining how an organisation collects, uses, and protects personal data.
- **Informed Consent**: Clear agreement provided by individuals, after being informed of the specific data processing activities.
- **Right to Be Informed**: The GDPR-mandated right for individuals to know how their data is being processed.
- **Data Breach Notification**: The requirement to notify affected parties promptly in the event of a data security incident.

Examples/Case studies

- **Case study 1**: A university introduces a new learning management system but fails to inform students about the data being collected. Complaints arise, prompting a review and public clarification of the system's privacy policy.
- *Lesson*: Always provide detailed information about new tools and their data collection practices.

- **Case Study 2**: A teacher uses a class chat platform and inadvertently shares a student's

TOOLS

TALKING PRIVACY & SAFETY

personal information. The student raises a concern, leading to training for educators on responsible communication practices.
- *Lesson*: Limit the sharing of personal data to essential information only.

- **Case Study 3**: An institution provides learners with unclear privacy notices. After a legal review, the notices are rewritten in plain language, leading to increased learner satisfaction and trust.
- *Lesson*: Use simple, concise language in all communications about data privacy.

ACTIVITY 2

Promoting Transparency and Trust in Data Handling

An adult educator collects data from learners through an online survey platform as part of a course evaluation. Learners raise concerns about the lack of clarity regarding how their responses will be stored, analysed, and shared. Some learners are hesitant to participate, citing privacy concerns and potential misuse of their information.

Step-by-Step Communication Strategies for Transparencying

Step 1
Provide Clear Explanations of Data Collection
- Clearly articulate why data is being collected, how it will be used, and the benefits for learners. For example, begin the survey with a statement such as, "This survey aims to improve course quality. All responses are anonymous and will only be used for educational purposes."

Step 2
Use Accessible Language for Privacy Policies
- Avoid technical jargon when explaining privacy policies to learners. Instead, use straightforward terms. For example, "data will be processed and stored in accordance with GDPR Article 6" with "Your data will be stored securely and used only for improving your learning experience."

TOOLS

TALKING PRIVACY & SAFETY

Step 3
Seek Explicit Consent Before Data Collection

- Request learners' agreement with a simple, opt-in format. For example, include a checkbox stating, "I agree to participate in this survey and understand how my responses will be used."

Step 4
Encourage Questions and Discussions About Data Privacy

- Define how long data will be stored and ensure unnecessary data is deleted after its purpose is served.

Step 5
Emphasise Learners' Rights

- Highlight learners' rights to access, correct, or request the deletion of their data. For example, share a one-page guide summarising these rights and contact information for further assistance.

Step 6
Ensure Transparency About Third-Party Tools

- Inform learners if third-party platforms are used for data collection or storage, and explain how these platforms comply with privacy regulations. For example, "We use [Survey Platform], which complies with GDPR, to ensure your data is securely stored."

Step 7
Regularly Communicate Updates and Changes in Data Practices

- Notify learners of any changes to data collection or storage policies. For example, send a brief email summarising updates, such as, "We have improved our data storage practices to further protect your privacy."

ACTIVITY 3

Fostering Learner Awareness and Engagement in Data Privacy

During an online course, learners are required to

TOOLS

TALKING PRIVACY & SAFETY

create user accounts on a collaborative platform to participate in discussions. Some learners express concerns about sharing personal information and their ability to control how their data is used. A learner asks about deleting their account and associated data after completing the course.

Six Key Steps for Engaging Learners in Data Privacy

Step 1

Transparency in Registration and Data Use

- Clearly communicate why personal information is collected and how it will be used. For example, at the beginning of the course, include a statement like: "Your account details are required to participate in this course. We ensure your data will not be shared without your consent."

Step 2

Promote Awareness of Learners' Rights

- Educate learners on their GDPR rights, such as data access, correction, and deletion. For example, provide a one-page summary of GDPR rights, or dedicate a short session to discussing these rights with learners.

Step 3

Provide Clear Opt-Out Options

- Ensure learners can opt out of optional data-sharing activities, such as participation in public discussions. For example, use checkboxes to allow learners to decide whether their profile is visible to other users on a platform.

Step 4

Encourage Learner Involvement in Data Practices

- Engage learners in discussions about how their data is handled, fostering a sense of ownership and understanding. For example, facilitate a group activity where learners evaluate a hypothetical data-sharing policy and suggest improvements.

TOOLS

TALKING PRIVACY & SAFETY

Step 5
Streamline Data Deletion Processes

- Make it easy for learners to request the deletion of their accounts and associated data. Share instructions, such as: "To request the deletion of your account, please email [support@institution.com] with your account details. Your request will be processed within 14 days."

Step 6
Incorporate Practical Exercises on Privacy Concepts
Use interactive activities to reinforce the importance of data privacy and safety. For example, host a quiz on data protection scenarios or discuss real-life examples of GDPR breaches and their consequences.

Examples/Case studies

Case Study 1: A course introduced a "Data Privacy 101" module during orientation, including videos and infographics about GDPR. Learners reported greater confidence in managing their data during the course.

Case Study 2: An educator organised a mock debate where learners argued for and against sharing specific types of personal data in educational settings. The interactive discussion-based activities encouraged critical thinking about data rights and responsibilities.

Case Study 3: A learning platform included a “Delete My Data” button that automated the data deletion request process. Learners appreciated the transparency and ease of control.

CHECKLIST FOR LEARNER ENGAGEMENT IN PRIVACY ISSUES

Pre-session

Prepare educational materials that explain

TALKING PRIVACY & SAFETY

GDPR principles and learner rights (e.g., infographics, short videos, or slides). Clearly communicate data usage policies during course registration, specifying how data will be stored, used, and protected.

Provide learners with opt-in consent forms for activities that involve data processing, such as recording sessions or sharing learner-generated content.

Set up secure platforms with encryption and password-protected access for course materials and activities.

During session

Reiterate learners' rights at the start of the session, ensuring they understand how to request access to or deletion of their data.

Facilitate discussions or activities to engage learners in exploring their data protection responsibilities and rights.

Avoid sharing sensitive information in group settings unless explicitly necessary and with consent from all parties involved.

Minimise data collection by requesting only essential information for participation in the session.

Post-Session

Follow up with learners by providing resources on GDPR rights and practices (e.g., links to helpful articles or guides).

Process data requests promptly, such as requests for data deletion or corrections.

Audit collected data and delete any information no longer necessary for educational purposes.

Document consent and compliance efforts to demonstrate adherence to GDPR principles.

TOOLS

TALKING PRIVACY & SAFETY

EMPOWERING EDUCATORS TO ENGAGE LEARNERS IN DATA PROTECTION

Empowering the Next Generation
10 rules for online privacy

This resource, developed by experts in education and privacy advocacy, offers educators practical tools and strategies to teach data privacy effectively. It provides lesson plans, interactive activities, and case studies that help learners grasp the significance of data protection in a digital world. The tool aligns with GDPR principles, focusing on key topics such as consent, transparency, and secure data practices. By using this resource, educators can empower learners to make informed decisions about their online presence and data privacy.

Enhancing Data Protection in Education
The compliance checklist for schools

This resource, provided by the Education Authority Northern Ireland (EA NI), is tailored to help schools and educators navigate GDPR compliance in educational settings. It offers detailed guidance on safeguarding personal data, addressing data breaches, managing data subject requests, and implementing secure data handling practices. Additionally, the tool includes templates and checklists that support schools in building a robust data protection framework. It is an essential reference for fostering transparency, ensuring lawful data processing, and promoting a culture of accountability in educational institutions.

TOOLS

ACCESS, REGISTRATION, ADMINISTRATION

Learner registration and user administration are essential processes in any educational system, particularly in online learning platforms or institutions that offer various courses and programs. These processes ensure that learners can successfully sign up for courses and that administrators can manage their profiles and access to different resources efficiently.

Adult Education Programme
User perspective: How to register and Enrol on our new website

This video tutorial provides a comprehensive walkthrough of a newly launched website for the adult education program. The presenter explains the website's features and registration process, focusing on making the user experience easier and more efficient based on feedback from students.

Adult Education Programme
Administrator perspective: to register and Enrol on our new website

In this video, viewers will be guided through the process of how a facilitator can register and invite a new Adult Student User to the Musical Ladder Portal. The video demonstrates the step-by-step procedure for setting up an adult learner's account, ensuring they can access all the features and tools available within the portal. It includes instructions on how to send an invitation to the new user and walk them through the registration process, making sure they are ready to begin their musical journey. Viewers are encouraged to subscribe to the channel to stay informed about all the new features and enhancements coming to the Musical Ladder Portal.

While the example focuses on the field of music, the theoretical tips shown in the video are equally relevant to the tool's broader functionality on "user administration."

TOOLS

ACCESS, REGISTRATION, ADMINISTRATION

THE EDUCATION PROGRAM REGISTRATION FORM GUIDE

Best Practices

Accurate Information is Key:

- Ensure all fields are completed with accurate and up-to-date information. Mistakes in basic details like your name, date of birth, or contact information can delay your enrollment or communication with the institution.

Double-check Contact Information:

- Check that your contact details are accurate. This will help the institution reach you if necessary.

Provide Full Educational History:

- *B*e honest about your highest completed education level. This helps educators tailor the learning experience to your academic background.

Disclose Special Needs or Accommodations:

- If you have any physical or learning disabilities, be sure to indicate this on the form. This will allow the institution to provide necessary accommodations and support.

Respect Confidentiality:

- Understand that your personal information is protected by privacy laws (FERPA). The institution may only share data as allowed for program evaluation or with testing organisations.

Practical Tips

Name and Contact Details:

- Tip: Always use your full legal name and ensure all contact information (email, phone number, and emergency contact) is correct. If you have any issues with your contact details, reach out to the institution's help desk.

TOOLS

ACCESS, REGISTRATION, ADMINISTRATION

Educational Background:

- Tip: Be truthful about your education level. Even if you completed education outside of the U.S., provide that information. If unsure about your highest grade or degree, check your transcripts or diplomas for reference.

Work Status:

- Tip: When selecting your work status, be honest about your current employment situation. Whether you're employed, seeking work, or not working, this helps the institution better understand your availability and support needs.

Special Accommodations:

- Tip: If you have a disability, fill out the section requesting accommodations. This may include extra time for assignments or accessibility tools. Be specific about what accommodations you may need.

Data Privacy:

- Tip: Carefully read the confidentiality section. You're asked to give permission for your information to be used for program evaluation and testing purposes. This ensures your data is protected, but also helps track your progress and provide you with the best learning experience.

Final Signatures:

- Tip: Before submitting, review the entire form for completeness. Make sure you've filled in every field accurately and signed where necessary. This will avoid delays in processing your enrollment.

ADMINISTRATION AND REGISTRATION CHECKLIST

Ensure the registration process complies with GDPR by collecting only the necessary personal data.

Provide learners with a clear privacy notice explaining how their data will be used and stored.

TOOLS

ACCESS, REGISTRATION, ADMINISTRATION

- *Secure documented consent from students for the use of their data, including any media (e.g., photos, videos) shared during the teaching process.*
- *Use a secure online platform for managing learner accounts and access permissions.*
- *Set up role-based access to restrict administrative privileges to authorised personnel only.*
- *Enable password policies requiring strong passwords and encourage learners to update them periodically.*
- *Regularly review and update learner account details to ensure data accuracy and relevance.*
- *Deactivate accounts of learners who are no longer enrolled or have completed their course.*
- *Use encrypted storage solutions for sensitive learner data, such as identification documents.*
- *Provide learners with access to their data and options to update or delete their information upon request.*
- *Inform learners about their rights concerning their data and the steps to report privacy concerns.*
- *Create a backup of learner registration data and store it securely in compliance with data retention policies.*

ACTIVITY 1

Case Study Discussions

Present a case study where user data was mishandled during the enrollment process. Have participants discuss the potential risks and how they could have been avoided with proper data privacy measures.

Role-playing

TOOLS

ACCESS, REGISTRATION, ADMINISTRATION

Divide participants into pairs, with one acting as an administrator and the other as a student. The administrator explains the data privacy policies during the enrollment process, ensuring that the student understands what data will be collected and how it will be used.

Methodological guidance:

Facilitate active participation

Engage learners in discussions around real-life scenarios to make them reflect on how data protection principles apply in adult education settings. Encourage them to share experiences from their institutions.

Simplify complex concepts

Data privacy laws can be complex. Break down the key principles (such as consent, data retention, and access rights) into simple, relatable terms. Use examples from their daily work in adult education to reinforce these concepts.

Encourage collaborative problem solving

Use group exercises to foster collaboration. For example, have learners develop a data protection checklist for the user administration process in their own institution.

Remember

Consent under GDPR must be freely given, specific, informed, and unambiguous. This means users need to actively opt-in to the processing of their data, not just be informed of it.

Definitions and Key Terms:

User administration

The process of managing user accounts and personal data within a system, including enrollment, updates, and deletion.

Data processing

The collection, storage, manipulation, and dissemination of personal data.

Data privacy

TOOLS

ACCESS, REGISTRATION, ADMINISTRATION

The protection of personal data from unauthorised access, use, or disclosure.

Consent
A key element of GDPR, referring to the voluntary agreement by a data subject to the processing of their personal data.

Data breach
An incident in which personal data is accessed, disclosed, or destroyed without authorisation.

Data retention
Data retention refers to how long personal data is kept. Institutions should establish clear retention periods for data and ensure that personal information is only stored as long as necessary for the purpose it was collected.

Examples/Case studies

Case Study 1: *GDPR compliance in enrollment*
An adult education center implements an online registration system where learners must review and consent to the data privacy policy before submitting their enrollment forms. This ensures that the center complies with GDPR's requirement for informed consent.

Case Study 2: *Handling sensitive data in a secure environment* - A vocational training provider uses a secure, encrypted database to store student enrollment data. Only authorised personnel can access the data, and students are informed of their rights to access, update, or delete their data upon request.

TOOLS

SECURITY IN EDUCATION TECHNOLOGY

The rapid adoption of educational technologies (EdTech) in schools and institutions has transformed teaching and learning experiences. However, it has also introduced significant challenges related to data privacy and safety. This topic focuses on identifying, assessing, and mitigating risks associated with the use of digital tools and platforms in education. By fostering education and awareness around data privacy and safety, schools and institutions can make informed decisions about integrating technology while prioritising the protection of their community's data.

UNESCO's Guidance on Data Privacy in Online Learning

UNESCO offers a comprehensive handbook titled "Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents." This resource provides strategies to safeguard personal information before, during, and after online learning sessions.

iKeepSafe's Data Privacy Curriculum

The Internet Keep Safe Coalition (iKeepSafe) has developed a curriculum focused on data privacy in education. It addresses concerns related to the use of educational technologies and offers guidance on protecting student personal information.

SPADATAS Project

The SPADATAS project aims to raise awareness about data fragility in educational settings. It provides tools and frameworks to protect the privacy, security, and confidentiality of student data, helping schools understand the implications of data-driven decision-making.

TOOLS

SECURITY IN EDUCATION TECHNOLOGY

eLearning Industry on Data Privacy

An article titled "Safeguarding Data Privacy and Security in eLearning" discusses the importance of data privacy in eLearning platforms. It outlines steps and best practices to ensure the safety and integrity of these platforms.

Privacy is key: Holding EdTech accountable

Common Sense Media evaluates popular EdTech platforms concerning security and the protection of students' right to privacy. Their insights help educators and parents make informed decisions about the tools they use.

Relevant Regulations / Standards

***ISO/IEC 27001**: An international standard for information security management systems, offering a framework for managing data safety in digital tools.*

Privacy Risk Analysis Exercise

Educators assess a specific educational tool, identify potential privacy risks, and suggest mitigations.
Example prompts: "Does this tool collect unnecessary personal information? How are learners' data stored and shared?"

Case Study Discussion

Analyze a real-life example of a data breach in education and discuss how it could have been prevente

Methodological Guidance:

Encourage open discussions about the balance between technological benefits and privacy concerns.

TOOLS

SECURITY IN EDUCATION TECHNOLOGY

Use visual aids (e.g., infographics) to simplify complex regulations for learners.

Provide real-world scenarios to connect theoretical knowledge to practical applications.

Definitions and Key Terms

Data Encryption
A method to secure information by onverting it into a code to prevent unauthorized access.

Phishing
A cyberattack that tricks individuals into providing personal information.

Examples/Case studies

Case Study 1: An adult education center adopted a learning management system (LMS) without reviewing its data-sharing policies. After a data breach exposed learners' personal details, the institution faced legal action and lost learners' trust. This illustrates the need for thorough technology vetting and compliance checks.

TOOLS

STORAGE AND PROCESSING

1. SECURE MAIL SERVICES

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.

- PROTON MAIL
- TUTANOTA

2. SECURE FILE SHARING

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.

- TRESORIT
- SYNC
- GOOGLE WORKSPACE

TOOLS

STORAGE AND PROCESSING

3. LMS SYSTEMS WITH SECURITY

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.

MOODLE CANVAS

4. SFTP FOR SECURE FILE TRANSFERS

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.

FILEZILLA WINSCP

5. DATA RETENTION AND DELETION TOOLS

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

TOOLS

STORAGE AND PROCESSING

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.

BLEACH BIT

ERASER

6. BACKUP AND RECOVERY TOOLS

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.

ACRONIS

VEEAM

TOOLS

DATA HANDLING & SECURITY

TACKLING DATA PROTECTION CHALLENGES

Practical steps to tackle key challenges in navigating data protection legislation

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.

Data Protection and Privacy Training

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.

Being Safe on the Internet

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.

TOOLS

DATA HANDLING & SECURITY

Minding the data: protecting learners' privacy and security

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.

CHECKLISTS

Securing online teaching:

- ✓ *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*

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*

TOOLS

DATA HANDLING & SECURITY

- *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*

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*

Post-session Privacy & 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

TOOLS

DATA HANDLING & SECURITY

Evaluate the session and note any privacy or safety issues to improve future sessions

ACTIVITY 1

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.

Pre-Session

Choose Secure Platforms: Use trusted tools like Zoom or Microsoft Teams. Ensure they are updated and configured with GDPR-compliant settings.

Minimise Data Collection: Only ask for essential information during registration (e.g., first name, email). Avoid collecting unnecessary personal details.

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.

Test the Platform: Familiarise yourself with features like muting participants, locking meetings, and enabling waiting rooms

During Session

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).

TOOLS

DATA HANDLING & SECURITY

Model Safe Practices: Avoid calling out full names or sharing personal information about participants. Refer to them by first name or aliases.

Engage Safely: Use interactive tools like polls or Q&A features to engage learners without requiring them to disclose personal information.

Monitor the Chat: Watch for and address any accidental sharing of sensitive details in the chat. Remind participants of privacy rules when needed.

Post-Session

Secure Materials: Save recordings, if any, in a password-protected folder and only share them with authorised individuals.

Provide Resources: Share a simple guide or checklist on staying safe online, tailored to the session's content.

Reflect and Improve: Note any privacy challenges during the session and adjust your approach for next time.

ACTIVITY 2

Relevant Regulations/Standards

ePrivacy Directive **-** Outlines rules for online privacy and data protection in electronic communications

Definitions and Key terms

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.

TOOLS

DATA HANDLING & SECURITY

Activities / Exercises 

Role-playing - Divide learners into groups to simulate common privacy risks (e.g., phishing emails or oversharing on social media) and discuss solutions.

Data Audit - Learners list the personal information they share online and discuss how to reduce their digital footprint.

Methodological Guidance 

Begin the session with a relatable story or case study to illustrate the importance of data privacy.

Use simple language to explain concepts and avoid technical jargon.

TOOLS

TRAINING & AWARENESS PROGRAMS

Training and awareness programs are essential for organisations to ensure compliance with data protection regulations such as the General Data Protection Regulation (GDPR) or other national and international laws. These programs educate employees, administrators, and other stakeholders on the importance of data privacy and security while fostering a culture of compliance. By prioritising education and awareness through well-structured training programs, organisations can effectively address data protection challenges and create a robust framework for compliance.

GDPR Data Privacy Professional (GDPR DPP) Training

Offered by DPO Europe, this course helps integrate GDPR requirements into information security strategies, ensuring data protection across IT infrastructures. It covers safe handling of personal data in compliance with GDPR.

Certified Data Protection Officer (CDPO) Intensive Training Course

Provided by DELTA Data Protection & Compliance Academy, this intensive online course equips individuals with the knowledge and skills to serve as Data Protection Officers, ensuring organisational compliance with GDPR.

Data Protection Officer (DPO) Online Training

InfosecTrain offers a comprehensive understanding of GDPR compliance, covering aspects such as organisational processes, privacy policies, consent mechanisms, and data protection impact assessments.

TOOLS

TRAINING & AWARENESS PROGRAMS

Global Privacy Awareness Training Program

TeachPrivacy offers a program designed to provide basic privacy awareness training to the workforce of global organisations, suitable for multinational corporations, including those based in the EU.

Data Protection Refresher and Advanced Course

EIPA offers a course designed to help refresh and update data protection knowledge, guided by experts and practitioners at the forefront of data protection.

KnowBe4 Security Awareness Training

EIPA offers a course designed to help refresh and update data protection knowledge, guided by experts and practitioners at the forefront of data protection.

SkillSoft Compliance Training

Skillsoft provides a wide range of compliance training courses, including data protection and privacy modules. Their content is designed to help organisations meet regulatory requirements and ensure employees understand their roles in maintaining data security.

OneTrust Privacy & Data Governance

OneTrust offers tools for data privacy management, including training resources to help organisations comply with global data protection laws. Their platform assists in managing consent, data mapping, and assessments, providing a comprehensive approach to data governance.

TOOLS

TRAINING & AWARENESS PROGRAMS

TrustArc Privacy Management Platform

TrustArc provides a suite of tools designed to help organisations manage privacy compliance. Their platform includes training modules, risk assessments, and data inventory management to ensure adherence to data protection regulations.

DataGuard Compliance Solutions

DataGuard offers comprehensive data protection and compliance services, including training programs tailored to organisational needs. Their solutions focus on integrating data privacy into business processes, ensuring continuous compliance with regulations like GDPR.

ACTIVITY 1

Relevant Regulations/Standards

ISO/IEC 27701: Advocates regular training as part of privacy information management systems.

National Laws and Codes of Conduct: Local adaptations of GDPR or specific data protection laws (e.g., DSGVO in Austria) often emphasize the need for employee education and awareness.

Data protection training: This is a dynamic area in adult education, focusing on equipping employees, trainers, and decision-makers with the knowledge to ensure compliance. Educators must integrate real-life scenarios, foster active engagement, and address learners' diverse professional contexts.

Definitions and key terms

Compliance - Adhering to legal and regulatory requirements.

TOOLS

TRAINING & AWARENESS PROGRAMS

Personal Data: Any information that can directly or indirectly identify an individual.

Data Minimization: Collecting only the data necessary for a specific purpose.

DPO (Data Protection Officer): A role mandated by GDPR for certain organizations to ensure compliance and act as a liaison with supervisory authorities.

Awareness Campaign: A structured effort to inform and educate employees about data protection practices, using posters, emails, or workshops.

Methodological Guidance

Utilize case studies and real-life examples to make concepts relatable and actionable.

Foster an interactive learning environment with discussions, role-playing, and scenario-based learning.

Provide simple checklists and templates to help learners apply the concepts in their workplaces.

Activities/Exercises

Compliance Workshop - Divide participants into groups and present case studies of data breaches. Groups discuss what went wrong and propose solutions to prevent future breaches. I.e., "What safeguards could have prevented the unauthorized access to customer data in this scenario?"

Interactive Role-Play - Participants simulate a data protection officer (DPO) conducting an internal training session, focusing on GDPR principles or responding to a data subject access request.

TOOLS

USE OF SOCIAL MEDIA APPS IN EDUCATION

Career-focused adults represent a promising market for higher education institutions facing declining enrollment from traditional students. However, adult learners often juggle multiple responsibilities and complex life circumstances, which can make enrolling in academic programs a daunting task. To support this demographic, it's crucial to streamline processes and remove barriers, including those linked to social media tools used in teaching. Simplifying information access, offering personalised support, and using user-friendly platforms can significantly improve adult learners' educational experiences.

Streamline Adult Learner Enrollment: Best Practices Guide

This guide outlines actionable steps to simplify enrollment processes and address barriers faced by adult learners. Strategies include providing clear and accessible information, rethinking application requirements, offering flexible deadlines, and improving transfer credit evaluations. Additionally, it emphasises the importance of intuitive technology, personalised guidance, and financial aid support, all aimed at making the enrollment process more inclusive and efficient for adult learners.

Maximising adult learner engagement in online environments

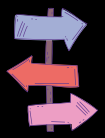
Skillrise, an initiative by ISTE (International Society for Technology in Education), provides a comprehensive framework to guide educators and institutions in creating engaging and effective digital learning experiences for adult learners. The tool outlines a structured approach to integrating educational technology, addressing factors such as readiness, team capacity, learner needs, and implementation strategies

USE OF SOCIAL MEDIA APPS IN EDUCATION

Using digital tools in teaching: Social Media

This video explores how social media and digital tools can positively impact academic settings, fostering engagement and enhancing learning experiences.
The content demonstrates practical ways to integrate social media platforms, collaborative tools, and creative media like podcasts into your teaching methodology. Learn how to inspire students and make the most of these digital tools to create interactive, modern learning environments.

USING SOCIAL MEDIA APPS FOR TEACHING PURPOSES GUIDE



Social media apps have transformed the way educators interact with students and deliver content. When used strategically in educational settings, these platforms can foster collaboration, creativity, and engagement. This guide will explore the best practices and practical tips for incorporating social media apps effectively into your teaching to enhance student participation and learning outcomes.

Best Practices

Choose the right platform for your audience:

- Not all social media apps are suitable for every educational need. Consider the age group, learning objectives, and privacy concerns when selecting a platform. For example, LinkedIn is great for professional networking and career-related content, while platforms like Instagram or Facebook can be used to share multimedia content and create interactive discussions.

Set clear guidelines and expectations:

- Establish clear rules about how social media

TOOLS

USE OF SOCIAL MEDIA APPS IN EDUCATION

should be used in the classroom. This includes how often students should post, what content is appropriate, and how to engage respectfully with peers. Setting these expectations from the beginning can help avoid misunderstandings.

Maintain professional boundaries:

- *Separate your personal social media presence from your professional* teaching accounts. This ensures that your students can engage with you in a learning-focused context while preserving your personal privacy

Integrate social media with learning goals:

- Ensure that the use of social media aligns with your educational objectives. Whether it's for discussions, group projects, or sharing resources, social media should have a clear pedagogical purpose to maximise its benefits.

Encourage collaboration and communication:

- Social media can facilitate peer-to-peer learning and collaboration. Create spaces for students to ask questions, share resources, and support each other. Encourage student-generated content, such as blog posts, videos, or infographics, which can deepen their learning experience.

Practical Tips

Select the right app for content sharing:

- Tip: If your goal is to share multimedia content, platforms like YouTube, Instagram, or TikTok can help you engage students visually. You can upload videos, tutorials, or live-stream discussions. Just ensure that videos are accessible and include captions if necessary.

Create private or closed groups:

- Tip: For more controlled communication, create private groups on platforms like Facebook or Discord. These spaces allow students to engage with each

USE OF SOCIAL MEDIA APPS IN EDUCATION

other without the concerns of public exposure. It also keeps discussions organised and focused.

Use hashtags for organisation:

- Tip: On platforms like Twitter and Instagram, use specific hashtags to organise content. This makes it easy for students to find relevant posts and follow course-related discussions. Encourage students to use the hashtag when posting course-related content to enhance visibility and interaction.

Encourage student contributions:

- Tip: Ask students to create and share content related to the subject matter. This could include sharing relevant articles, reflecting on class discussions, or posting their own creative works. Reward students for their contributions, fostering a sense of ownership and engagement.

Monitor and moderate:

- Tip: Keep an eye on social media interactions to ensure the environment remains respectful and conducive to learning. Regularly monitor posts for inappropriate content, ensure students are following guidelines, and address any issues swiftly.

Incorporate live interaction:

- Tip: Use live streaming tools like Instagram Live, Facebook Live, or YouTube Live to host Q&A sessions, guest speakers, or real-time discussions. This creates an interactive space where students can engage directly with the content and the educator.

Create polls and surveys:

- Tip: Use platforms like Twitter or Instagram Stories to create quick polls or surveys related to class content. This can be a fun, engaging way to gather feedback or check understanding.

TOOLS

USE OF SOCIAL MEDIA APPS IN EDUCATION

CHECKLISTS

Secure online teaching session
Step-by-step

- *Verify that the social media app complies with GDPR by reviewing its privacy policy and data-handling practices.*
- *Adjust the app's privacy settings to restrict access to teaching materials and interactions only toenrolled students.*
- *Secure documented consent from students for the use of their data, including any media (e.g., photos, videos) shared during the teaching process.*
- *Create private groups, chats, or spaces within the app for secure and controlled discussions.*
- *Ensure all shared teaching materials, posts, or media are free from personal identifiable information (PII).*
- *Set up strong passwords and enable two-factor authentication (2FA) for accounts linked to teaching purposes.*
- *Monitor and moderate group activities to prevent data breaches or misuse of the platform.*
- *Encourage students to use privacy-focused profiles or pseudonyms if they have concerns about data exposure.*
- *Review and delete unnecessary files, private messages, or temporary data from the app after each session.*
- *Avoid sharing sensitive or personally identifiable information (PII) on the platform, such as addresses or full names.*
- *Inform students of their rights regarding data privacy and explain how their information will*

TOOLS

USE OF SOCIAL MEDIA APPS IN EDUCATION

be used. Prepare a contingency plan for data breaches, including steps to notify affected individuals and mitigate risks

Are you using social media effectively for learning?

I understand how using social media can enhance my learning and make it more interactive.

I have chosen the social media app(s) that best fit my learning goals and preferences.

I feel confident about protecting my privacy and know how to adjust settings to stay safe online.

I know the ground rules for respectful and productive online discussions.

I can share ideas, projects, or questions in a way that contributes to group learning.

I participate in polls, quizzes, or challenges to make learning more fun and dynamic.

I use hashtags or group tags to find relevant posts and keep everything organised.

I am comfortable asking for help or clarification if I don't understand something on the platform.

I reflect on how social media activities connect to my personal learning goals.

I give feedback on what works or doesn't so that everyone benefits from a better learning experience.