

Security and Privacy in Academic Data management at Schools SPADATAS

2022-1-ES01-KA220-SCH-000086363



SPADATAS
Security and Privacy in Academic Data
Management at Schools



**Co-funded by
the European Union**

Understanding the privacy concerns of AI and LLMs in schools

HUMAN ENVIRONMENT RESEARCH GROUP – TECHNOLOGY ENHANCED LEARNING
Universitat Ramon Llull (URL) – Universidad de Salamanca (USAL)
SPADATAS CONSORTIUM



**Co-funded by
the European Union**

The SPADATAS project (Ref.: 2022-1-ES01-KA220-SCH-000086363) is co-funded by the European Union. The content of this publication is the sole responsibility of consortium and neither the European Union, nor the Spanish Service for the Internationalization of Education (SEPIE) are responsible for the use that may be made of the information disclosed here.



<https://creativecommons.org/licenses/by-nc-sa/4.0/>

The use of Large Language Models (LLMs) and AI tools that rely on prompting is becoming increasingly popular in educational settings. These tools can generate content, answer questions, and even assist with complex subjects, such as ChatGPT. However, their functioning often involves collecting personal data from users, especially when inputs include sensitive information like names, locations, or personal thoughts. This data, although used to improve responses, may expose students to unintended privacy risks.

Data fragility becomes a concern when personal or sensitive data is stored and processed by AI systems. These systems may not always guarantee complete security, making the stored information vulnerable to cyberattacks or unauthorized access. Even when data is anonymized, the risk of re-identification through advanced techniques can lead to breaches of confidentiality and personal privacy.

Confidentiality and privacy risks

As students interact with LLMs and AI tools, they **may unknowingly provide personal details** that could be stored and processed by third-party servers. This raises questions about data confidentiality:

- Who has access to this data?
- Are there safeguards in place to ensure that sensitive information remains private?

In educational environments, where children and teenagers use these tools, protecting their data becomes a paramount responsibility.

Privacy concerns also extend to how data is shared and processed. Many LLMs are cloud-based, meaning that user inputs may travel through different networks and servers. If these networks are not secure, data can be intercepted or misused, putting students' personal information at risk. Schools need to ensure that robust privacy protocols are in place before integrating AI tools into their teaching practices.

Security and data protection measures

In addition to privacy concerns, security threats loom large with AI tools. Without adequate security measures, these systems can be susceptible to hacking or unauthorized use, leading to significant data breaches. For schools, this means that students' personal information, academic records, or even casual conversations with AI could be exposed. It is crucial for educational institutions to evaluate the security infrastructure of AI tools and adopt best practices for data protection.

Schools must also **educate students** on responsible use. Encouraging students to **avoid sharing personal information** and teaching them about the potential risks of using AI tools will help mitigate these concerns. By raising awareness and implementing secure practices, schools can create a safer learning environment for everyone.



Co-funded by
the European Union

The SPADATAS project (Ref.: 2022-1-ES01-KA220-SCH-000086363) is co-funded by the European Union. The content of this publication is the sole responsibility of consortium and neither the European Union, nor the Spanish Service for the Internationalization of Education (SEPIE) are responsible for the use that may be made of the information disclosed here.

Key points

1. LLMs and AI tools collect personal data through user prompts, raising privacy risks.
2. Data fragility refers to the vulnerability of personal information to breaches and unauthorized access.
3. Confidentiality is compromised when personal data is processed without secure protocols.
4. Privacy concerns arise when data travels through unsecured networks and is shared with third parties.
5. Schools should educate students on responsible use of AI tools.



**Co-funded by
the European Union**

The SPADATAS project (Ref.: 2022-1-ES01-KA220-SCH-000086363) is co-funded by the European Union. The content of this publication is the sole responsibility of consortium and neither the European Union, nor the Spanish Service for the Internationalization of Education (SEPIE) are responsible for the use that may be made of the information disclosed here.