Data Privacy and Security

📘 Stop and think

The data (both test data and user login information) is sensitive and requires careful consideration because of privacy concerns and also potential legal implications. [1]

🚩 Clarify goals

As we mentioned in the overview page, the main goal is protecting sensitive personal and performance data within user profiles and test submissions. What's more, the team should also think about balancing the need for functionality when ensuring data privacy.

💡 Determine known and unknown facts

Known	Unknown
Encryption enhances security.	How encryption will affect the functionality of our application?
Using plain data makes more focus on functionality.	The specific requirements for data protection laws.
	How many awareness that user know about their data may have the risk of privacy.

🌈 Develop options

Options
Keep the data plain.
Data categorisation and encryption.

⤴️ Consider foreseeable results of the options

Option 1 may make the development easier and focus more on the functionalities. But this will pose a risk to data privacy, security, making the system vulnerable and also break the reputation of the team members.

Option 2 may require more efforts and also resources and may lead the development more complex, but it will maintain the data security and the system will be more reliable.

📝 Refer to a code of ethics for guidance of areas to be mindful of

Our team using the Engineers Australia ethics [2] as the guidance in this ethic consideration. Regarding to 4.1, we should be sensitive to public concerns (which is data privacy) and also we should inform employers or clients of the likely consequences of proposed activities on the community and the environment. In this case, we will try to reduce the risk and also we will inform this to the client.

ℹ️ Consult with respected staff or outside professionals

As some of the team members are doing internship in this semester, so we ask some supervisors about this concern and decided the following actions based on their suggestions.

✅ Decide the course of action and take it

Options
Find the less amount of necessary data which need to contain in the system
Put the privacy alert in the ‘help page’ to make sure the user used this application are willing to provide their personal data.
Implement different access authority for different roles
Implement strong encryption for data storage

📚 Reference

[1] Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013, April). Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 3393-3402).

[2] Engineers Australia. (2022). Code of Ethics and Guidelines on Professional Conduct. https://www.engineersaustralia.org.au/sites/default/files/2022-08/code-ethics-guidelines-professional-conduct-2022.pdf