MONASH University

Monash Tutor Allocation System

Technical Report: Privacy Audit

FIT3170: Software Engineering Practice

Submitted by Malaysia Team

Stuart Boey Chie Sheng - 29519985
Ahmed Nassar - 28901797
Teo Wei Han - 30242711
Cheong Chee Feng - 30222397
Ong Jeng Yue - 29637996

Submitted on January 3, 2021

Executive Summary

This technical report is about the privacy audit that our agile team performed on the Monash Tutor Allocation System. Our team consulted the Australian Privacy Principles and Information Privacy Principles to identify privacy issues in the system.

It is found that we should improve the security of the system by implementing multi-factor authentication during user login and employ encryption for our database. Besides, we need to implement a user de-identification functionality. Privacy policy that clarifies the use of unique identifiers in our system needs to be prepared and collection notice by Monash University should inform the users that their data will be used in this new system.

To allow users access to their personal data, we should provide a support contact number or online request ticket for users to request access to personal data. A setting page will be needed for the users to ensure their data is always up-to-date, accurate and complete.

Due to the nature of new requirements involving more research and development, it is possible that a delay on the delivery of the project is expected.

Table of Contents

1.0 Introduction *3*
2.0 Consulted Privacy Principles *4*
3.0 Type of Personal Information Collected *6*
3.1 Personal Information: **6**
3.2 Network Privacy Information: **6**
3.3 Career Related Sensitive Information: **6**
4.0 Privacy Related Issues and Suggested Solutions *7*
4.1 Issue 1: Overall Security of the System **7**
4.2 Issue 2: De-identification of Personal Information **8**
4.3 Issue 3: The Use of Unique Identifiers **9**
4.4 Issue 4: Awareness on the Collection and Use of Personal Information **9**
4.5 Issue 5: Access to Personal Information **11**
4.6 Issue 6: Accuracy and Correctness of Personal Information **11**
5.0 The Impact on Timely Delivery of the Project *12*
6.0 Conclusion *13*
References *14*
Appendix ..... *A*
Team Contribution ..... *A*

List of Tables and Figures

Table 6.1: List of Issues and Solutions **13**

1.0 Introduction

With the development of the Monash Tutor Allocation System, we have been focusing on functional requirements of the system but not the privacy requirements, it is important that our application meets the privacy requirements to protect the information of our users and their privacy rights. The purpose of this report is to investigate the privacy policies and legislative requirements relevant to the application so that we can make changes to the requirements of our application to meet these policies and requirements.

In this report, we will first identify privacy policies and regulations that are relevant to our system. Then, a list of key types of information collected, used and stored by the system that are covered by these policies and regulations will be presented. We will then identify a list of issues that we need to address due to the change of requirements by referencing the privacy policies and regulations and try to come up with solutions for the issues. Lastly, analysis of the impact of these issues on the timely delivery of this project will be done.

This report will not cover aspects of the system that already adhere to the privacy policies and regulations. Besides, privacy policies and regulations outside of Australia will not be covered as well because this system is intended to be used in the Faculty of Information Technology Monash University Australia for now.

2.0 Consulted Privacy Principles

After researching several reputable sources to investigate the privacy principles and regulation under the establishment of software within the Australian sovereignty, it has been found that the laws and regulations correspond to certain general principles around collecting and disclosing personal information, an organization's governance and accountability, the integrity of personal information, and finally, the rights of access to these personal information [1].

The corresponding laws and principles are achieved from the acts established by both Australian Officer of Information Commissioner - Australian Privacy Act 1988 (Commonwealth) and Officer of the Victorian Information Commissioner - Privacy and Data Protection Act 2014. Both legal guidelines and principles establishment correspond to the same objectives. After carefully considering and studying both sources, a summary of the findings of principles from both sources can be found listed below. Do note that the term APP corresponds to the 13 principles established under Australian Privacy Act 1988[1] and the term IPP corresponds to 10 principles established by Officer of the Victorian Information Commissioner under Privacy and Data Protection Act 2014 [2].

2.1 Both APP principle 1 [1] and IPP principle 5 [2] state that the entity is to ensure personal information is managed in an open and transparent way

2.2 Both APP principle 2 [1] and IPP principle 8 [2] state that the entity should provide, with limited exceptions, the choice for anonymity or the use of a pseudonym to the provider of the information

2.3 Both APP principle 3 [1] and IPP principle 10 [2] state that the entity should understand the circumstances in which they are allowed to collect sensitive information such as political alignment, religious views, sexual orientation, or criminal records, and take reasonable and proper measures to ensure the protection and containment of the collection of such solicited information.

2.4 APP principle 4 [1] discusses the actions and steps to be taken by the entity upon the receival of unsolicited information.

2.5 APP principle 5 [1] states that the entity should disclose their intention of collecting information, and provide an explanation on how these information will be used

2.6 APP principle 6 [1] discusses how an entity may use or disclose personal information and under what conditions or expectations.

2.7 APP principle 7 [1] states that the entity should avoid the use or disclosure of personal information and data for the purpose of direct marketing without consent from the provider of such data

2.8 Both APP principle 8 [1] and IPP principle 9 [2] discusses the actions and steps an entity must take to protect personal information before it gets disclosed overseas, so that the overseas recipient does not breach the respective principles.

2.9 APP principle 9 [1] states that the entity should understand the limited circumstances of the adoption of a government related identifier as its own identifier.

2.10 Both APP principle 10 [1] and IPP principle 3 [2] state that the entity should take reasonable measures to ensure the integrity, validity, and authenticity of the data at all times

2.11 Both APP principle 10 [1] and IPP principle 4 [2] state that the entity should take reasonable measures to avoid the misuse, interference, loss, and unauthorized access to personal information and data.

2.12 Both APP principle 12 [1] and IPP principle 6 [2] states that the entity should provide and protect the right of access and correction of the information provided by the owner

2.13 IPP principle 1 [2] states that the entity should collect only the necessary information by rightful and lawful means, and provide an explanation on how or why such collected information will be used

2.14 IPP principle 2 [2] states that the entity can only use the information collected for the outlined intention, and should refrain from disclosing the information without prior consent

2.15 IPP principle 7 [2] states that the entity should understand the circumstances for the permission to use a unique identifier and the extent of the necessity for the permission to be granted.

3.0 Type of Personal Information Collected

After exploring the Australian privacy laws and regulation established by both Australian Privacy Act 1988 and Privacy and Data Protection Act , the team has further investigated the software in development, Monash Tutor Allocation System, to uncover the nature and type of the personal and private information that will be collected by the workforce team and operators of the system. This was done to evaluate the findings against the list of laws and regulation concluded regarding privacy under the Australian Government Department of Information Commissioner.

The investigation lead to the identification of the following key types of information that will be collected, used, and stored by the system:

3.1 Personal Information:

3.1.1 The full name of staffs that are either full-time or part-time employed under Monash University

3.1.2 The location of their work, and most likely, their residence, in the form of the university campus, identified by the name of the city

3.1.3 Contact information in the form of the staff's email address

3.2 Network Privacy Information:

3.2.1 The private credentials used to login into the system

3.3 Career Related Sensitive Information:

3.3.1 The working hours of a staff member

3.3.2 The working days of a staff member

3.3.3 The role or position of a staff member

These information are all covered by the laws and regulation mentioned in the prior section, and adequate steps and measure must be developed and deployed to ensure the compliance to the Australian privacy law governing the information and data of such type, ensuring the protection, integrity, and authenticity of them without compromising the privacy, safety, and rights of Monash University staff members.

4.0 Privacy Related Issues and Suggested Solutions

4.1 Issue 1: Overall Security of the System

Among the 10 principles from the Information Privacy Principle(IPP), principle 4, revolving around data security, is a prioritised issue that we have identified. This is in line with the client's request to ensure that the data is kept securely at all times. Point 1 of principle 4 states that "An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure"[3]. Considerations in regards to what can be deemed reasonable must take into account the "risk of harm to the people the information is about, the cost and difficulty of implementing the security measure and the damage to the organisations that might result from a failure of security or a breach"[3]. Thus the reasonable steps stated in the guideline should be "proportionate, appropriate and relevant to the risk of harm to the individual"[3]. This is an important distinction to make as perfect security is impossible. Our application holds various kinds of personal information such as email addresses, education level and others. Within our application, the steps that have been and will be applied to protect this personal information can be said to be only the bare minimum. At the user-facing application where the information is displayed, there is only a simple password protection. Currently, access to the third-party database we use, PostgreSQL, has not been secured in any way beyond a simple password protection as well.

For the security of the user-facing application, our team is in the midst of implementing a role-based access control which would strengthen the data security of the application so that only authorized users have access to personal information. However, this would not be fully sufficient. A straightforward way to further protect the personal information that will be on display within the application is to use multi-factor authentication. This has already been implemented in quite a few applications within the Monash software ecosystem and should likewise be implemented here due to the sensitivity of the data displayed. The advantage to this method is that it is a straightforward, well-established and well-documented method that is still very effective as it makes obtaining access to an account twice as hard than just relying on a password. Furthermore, since this method has been applied in many Monash software applications, it will not be an additional burden to end-users in terms of time and energy spent learning how to use it. The only disadvantage is the time, effort and cost it takes to implement this functionality.

In terms of the data security of the database, steps need to be taken to secure the PostgreSQL database that we use. This is because although PostgreSQL is an established open-sourced database, it has 112 known security vulnerabilities, as per CVE[4].The simple way to resolve this in the future would be to have the database hosted on an Amazon Relational Database Service (RDS) which would be connected to an Amazon Elastic Compute Cloud(EC2) where the website is hosted on. It would be more secure by implementing features such as encrypting all the underlying data within the database and its automated backups using keys managed by AWS Key Management Service (KMS)[5]. Another feature it provides for security is to isolate the database instances in its own virtual network using Amazon Virtual Private Cloud (VPC)[5]. This prevents external malicious attacks on the database. However, the major disadvantage to this solution is the extra cost needed to acquire these services. It would also take more time and effort to learn, implement and maintain all these various services.

Currently there are various other ways to secure the database. One way is to use physical separation to isolate datasets that can be kept apart[6]. By using tools such as pg_hba and role-based access control(RBAC), we can control access to the physically separate database. While this has the benefit of preventing datasets to be viewed or compromised simultaneously, the major disadvantage is that it prevents SQL joins. Another way is by using encryption for all values that do not require to be decrypted[6]. PostgreSQL itself has various options for encryption which includes encrypting data across a network, ssl host authentication, client-side encryption and others[7]. This provides an additional layer of security, should the database be compromised. This is because the data within the database would not be unencrypted, preventing it from being used in any form or manner. On the other hand, it also means extra computing overhead to encrypt all the data that enters the database.

Besides that, to monitor this issue, we can use the “pg_stat_statements”[8] from PostgreSQL which can allow the tracking of all queries executed within the database. This allows a trail to be left to identify culprits who intend to misuse the data. The disadvantage of this is that it requires additional shared memory and also to restart the server when the module is added or removed[8].

Overall the recommendation for the next steps for this issue is to add multi factor authentication for the user-facing application and to use encryption for the database to ensure all personal information within is protected. In the future, when the system is hosted on AWS, the security features for the Amazon RDS should also be added. “pg_stat_statements” should also be used within the database to allow for monitoring of all accesses of the database.

4.2 Issue 2: De-identification of Personal Information

Another issue is point 2 of principle 4 which states “An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose”[3]. This is an issue because as of now, there have been no plans or discussions to configure the system to allow for the ability to “destroy or permanently de-identify personal information”[3].

However this issue has a relatively simple and straightforward way to fully address it which is to make resolving it a task within the development of the system. Adding the functionality to remove data from the system is a very common functionality and easy to implement. This can be done by either setting up a page on the application to remove data or to directly access the database and remove it. Permanently de-identifying personal information may be slightly more challenging as research into how to de-identify personal information would have to be conducted. However, implementing it should be relatively straightforward as well. A thing to note when going with this option is that de-identified personal information can be reidentified if other information can be matched with it[3].So if the option is to de-identify personal information, Monash must monitor the information to ensure that the data is in a sufficiently de-identified form and safe from reidentification.

A way to monitor this issue is to verify in the database whether the data has been either de-identified or destroyed. Using “pg_stat_statements”[8], which was mentioned before, is also an option to monitor whether the delete or update query was applied correctly.

Between the two options, destroying the personal information when no longer needed would be the recommended approach as it ensures the security of data and is simpler to conduct and maintain. In terms of monitoring, accessing the database and verifying is what we recommend.

4.3 Issue 3: The Use of Unique Identifiers

A current issue we have on hand is the usage of unique identifiers in the database to store personal information of Monash staff such as their email address, availability etc. According to the Information Privacy Principles of the Office of the Victorian Information Commissioner [9], under Principle 7, it states that "An organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.". According to Principle 7, use of unique identifiers is prohibited unless necessary, in our case the use of unique identifiers can be avoided at the cost of the system's efficiency. Hindering the efficiency of the system is currently out of the question as our client is insistent on an efficient system. Therefore other forms of resolution must be considered while addressing this issue.

Point 7.22 of Principle 7 states that "The potential privacy risks associated with profiling and data matching increase when a unique identifier assigned by one organisation is adopted by other organisations. To minimise these risks, IPP 7.2 limits the adoption of identifiers across multiple agencies.". This point does not introduce any issue to our current system as the unique identifiers that are used are generated by our system itself. Point 7.33 of Principle 7 also notes that "IPP 7.3 prohibits an organisation from using or disclosing a unique identifier assigned by another organisation, unless one of the following applies". This point does not introduce any issues with our current system as well as the unique identifiers are currently only used within the system. However, if the system is to be expanded in the near future to integrate with other systems, this point must be revisited.

Going back to the matter at hand, a feasible solution to the issue brought upon by Principle 7 would be to very clearly list out the organisation's usage of unique identifiers within the system in a privacy policy agreement form. The privacy policy agreement template can be found and downloaded at the Business portal of Australia [10]. The privacy policy agreement can then be included in the Terms of Service [11] agreement of the organisation. Google's Privacy Policy statement [12] on unique identifiers can be used as an exemplar on how this could be done. This proposed solution will bring about and address any issues that are brought upon by the use of unique identifiers in our current system as users will be made aware of this upon enlistment.

4.4 Issue 4: Awareness on the Collection and Use of Personal Information

An additional issue that we have to consider is the collection of data in our system. According to the Information Privacy Principles of the Office of the Victorian Information" Commissioner [9], under Principle 1, Point 1.50 , it states that "IPP 1.3 requires organisations to take reasonable steps to make individuals aware of the identity of the organisation and how to contact it, the fact they may access that information, the purposes for which the information is or was collected, the names (or types) of organisations or individuals to whom the information is usually disclosed, any law requiring the

collection and the main consequences (if any) if the person does not provide any or part of the information.". As of now, the system does not deal with any legitimate personal information. However, the system is expected to be integrated with Monash's existing systems, and the data that is needed by the current system will most likely originate from Monash's databases. To fully address the matters brought upon by IPP 1.3, it is crucial that Monash is prompted upon this privacy issue when the system is handed-over. They must then take any legal steps required to ensure that the individuals are aware of their data being used in a new system. This could be done with Collection Notices as stated by the Office of the Victorian Information Commissioner [13].With the proposed solution mentioned above, Monash will ensure that the newly integrated system fully abides by the law of privacy and data protection set by the Victorian state government.

As the system will be handed over to Monash themselves, IPP 1.2, IPP1.4 and IPP 1.5 of Principle 1 should not be an issue as these points should already have been handled by Monash previously during initial collection of information for their existing systems. As for IPP 1.1, the current system does not collect any personal information that is unnecessary, thus no real issue is brought upon by this.

Besides that, the Use and Disclosure Principle and Openness Principle of the Privacy and Data Protection Act also have been completely violated as the data subjects are not informed how their information collected by the organisation is being used or disclosed and how are they able to access their personal data and ensure the information is correct. According to the Information Privacy Principles of the Office of the Victorian Information Commissioner [9], in IPP2 [14], it says that "An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless..." and the Openness Principle which is IPP5 [15] stated that " An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.".

As mentioned before, our current system is missing the policy and statement to ensure that the users are being informed that their data and information are collected for the primary purpose. If the organisation is required to use those data and information for other purposes, they must make sure that it does not violate the primary purpose of collecting the users data and information. This policy can be documented to allow users to read through it so that they know what sort of personal information is being held, for what purposes, and how those information are collected, held, used and disclosed.

Therefore, the solution to this is that we can have a policy document that relates to data protection including the collection notice which can be implemented when the user first uses the application. The policy will also mention how the organisation will manage those personal information which was stated in IPP5.1 [15]. The users have to read through some stated policies and agree with it before they are allowed to proceed on using this system.

4.5 Issue 5: Access to Personal Information

Right now our system might be using the user data for some algorithm for some calculation purposes but we are not displaying those information to them. So they also have the right to access those information that we have collected. If they want to access all the information that we store about them, we need to provide it to them. The user can only access their own information. If the information they requested has the possibility to harm or impact another person, the organisation has the right to reject the request as listed in IPP6.1(a) and IPP6.1(b) [16]. The user also has the right to make corrections of their information held by the organisation as stated in IPP6.5 [16]. However, the organisation also has the right to reject the correction and provide the reason to the user.

So, to allow users to be able to access all of their information, we can provide them with a support contact number or have an online request ticket for them to make requests to obtain their information that is stored by our system. Next, the user will be able to check that if their information held is accurate, if it is not accurate, they can request for correction by filling up the correct information.

4.6 Issue 6: Accuracy and Correctness of Personal Information

The next issue in our system is the data integrity has a poor standard which can be improved in the future. This issue violates the third principle in the Information Privacy Principles of the Office of the Victorian Information Commissioner [9], the Data Quality Principle and APP 10 of the Office of Australian Information Commissioner [17] . The Data Quality Principle stated “An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date”. Our current system obtains the data from the Monash’s database and those data have to be updated manually. If there are changes being made in the Monash’s database, our current system does not update synchronously.

Since there is no update being done synchronously, so those data we are using are not accurate which means that our system also violates the sixth principle which is Access and Correction Principle under point 6.48 in IPP6.5 [16]. The point 6.48 stated that “If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date”. So, our system might not show the latest data and information to the end user.

To address this issue, we can implement a profile setting page to allow users to change their personal information, such as unit preferences and availability. For example, if a TA found out that he or she selected too many units in the preferences list, then the TA can remove some of the units or the TA can change their total working hours in the availability if they do not want to work too much. TAs are given time for them to change the unit preferences and availability. After that period, they should not be able to change anymore since offers are being finalised and delivered.

5.0 The Impact on Timely Delivery of the Project

With 6 of the issues mentioned above, it is expected that issues regarding the security of the system will have the highest impact on the timely delivery of the project, this is due to the fact that more research needs to be done on the encryption of the database to ensure that it is done correctly and efficiently. The integration of a multi-factor authentication system to the current google authentication system will also need to be studied.

Functionality for users to de-identify themselves should be straightforward to implement but research into how to do it correctly will also be needed. Besides, we would need to communicate with our stakeholders about the de-identification of a user as the data in our system might be needed for some purpose.

A setting page for the user's personal information would have the next highest impact on the delivery of the project. While implementing this functionality should be uncomplicated, we would need to communicate with our stakeholders regarding the mechanism for the user to change their preferences and information .

These requirements were not considered before this privacy audit, with PI3 having planned out with 8 tasks and 2 more tasks to be brought forward from PI2, is it possible that these additional issues will cause a delay on the delivery of the project.

The other issues surrounding the privacy policies, use and access to personal information should be able to be solved relatively quickly, therefore, should have minimal impact on the timeline.

6.0 Conclusion

After investigating the privacy policies and regulation that are relevant to our system, the 13 Australian Privacy Principles (APP) from the Privacy Act 1988 and the 10 Information Privacy Principles (IPP) from the Privacy and Data Protection Act 2014 (Vic) are used as the guidelines for the privacy requirements of our system. The issues that we identified and the possible solutions are summarised in table 6.1. By implementing the solutions that we suggested, users' information and users' privacy rights should be better protected

Table 6.1: List of Issues and Solutions

Issue	Solution
Overall Security of the System	• multi-factor authentication for the user-facing interface. • Encryption for the database
No way for the users to de-identify themselves	• Implement a function for the user to de-identify themselves
Unique identifiers are used to identify the users of the system	• List out the organisation's usage of unique identifiers within the system in a privacy policy agreement for
User might not be aware that their information will be used in this system by Monash University	• Collection notice by Monash University should inform users that their information will be used in this system
User do not have access to all the personal information stored about the user	• Provide support contact number or online request ticket for the users to request access to all the information stored about them in the system
Personal information in the system may not be accurate, up-to-date and complete	• Provide a setting page that allows the user to change their personal information

A delay on delivery of the project is expected with the new requirements for better security of the system, user de-identification and ability for users to update their personal information.

References

[1] Office of Australian Information Commissioner. "The Australian Privacy Principles". OAIC. https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/ (Accessed Dec, 27, 2020).

[2] Office of the Victorian Information Commissioner. "Short guide to the Information Privacy Principles", OVIC. https://ovic.vic.gov.au/wp-content/uploads/2018/07/Short-guide-to-the-IPPs-.pdf (Accessed Dec, 27, 2020.

[3] Office of the Victorian Information Commissioner. "IPP 4 – Data Security", OVIC. https://ovic.vic.gov.au/book/ipp-4-data-security/ (Accessed Jan. 1, 2021)

[4] CVE Details. “Postgresql: Security Vulnerabilities.” CVE Details. https://www.cvedetails.com/vulnerability-list/vendor_id-336/product_id-575/Postgresql-Postgresql.html (Accessed Dec. 26, 2020).

[5] Amazon Web Services. “Amazon RDS for PostgreSQL features”, AWS. https://aws.amazon.com/rds/postgresql/features/ (Accessed Jan. 1, 2021).

[6] UpGuard Team. “How to Secure Your PostgreSQL Database - 10 Tips.” UpGuard. https://www.upguard.com/blog/10-ways-to-bolster-postgresql-security (Accessed Dec. 26, 2020).

[7] PostgreSQL. “16.6. Encryption Options.” PostgreSQL 8.1.23 Documentation. https://www.postgresql.org/docs/8.1/encryption-options.html (Accessed Dec. 26, 2020).

[8] Takahiro Itagaki. “F.29. pg_stat_statements.” PostgreSQL 9.4.26 Documentation. https://www.postgresql.org/docs/9.4/pgstatstatements.html (Accessed Dec. 26, 2020).

[9] Office of The Victorian Commissioner. Privacy and Data Protection Act 2014. https://ovic.vic.gov.au/privacy/guidelines-to-the-information-privacy-principles/ (Accessed Dec. 25, 2020)

[10] Business Victoria. Privacy Policy Template Update 2017. https://www.business.vic.gov.au/__data/assets/word_doc/0011/1113599/BV-Privacy-Policy-Template-Update-2017.docx (Accessed Dec. 25, 2020).

[11] Upcounsel. “What are terms of services?”. Upcounsel. https://www.upcounsel.com/what-are-terms-of-service (Accessed Dec. 25, 2020).

[12] Google. Google Privacy and Terms. https://policies.google.com/privacy/archive/20180525-20190122?hl=en (Accessed Dec. 25, 2020).

[13] Office of the Victorian Commissioner. “Collection Notices”. OVIC. https://ovic.vic.gov.au/book/ipp-1-collection/#IPP_1.3:_Collection_notices (Accessed Jan. 1, 2021).

[14] Office of the Victorian Information Commissioner. "IPP2 - Use and Disclosure”. OVIC. https://ovic.vic.gov.au/book/ipp-2-use-and-disclosure/ (Accessed Jan. 2, 2021).

[15] Office of the Victorian Information Commissioner. "IPP5 - Openness”. OVIC. https://ovic.vic.gov.au/book/ipp-5-openness/ (Accessed Jan. 2, 2021).

[16] Office of the Victorian Information Commissioner. "IPP6 - Access and Correction”. OVIC. https://ovic.vic.gov.au/book/ipp-6-access-and-correction/ (Accessed Jan. 2, 2021).

[17] Office of the Australian Information Commissioner. "APP 10 — Quality of personal information". OAIC. https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information/ (Accessed Jan. 1, 2021).

Appendix

Team Contribution

Tasks and Time Tracking For Technical Report 2			
Name	Task done	Time Spent (hours)	Notes
Stuart	Writing up 2 issues	3	
	Meeting discussion	1	Report Discussion
	Revision to suggestion by teammates	1	
	Total Hours	5	
	Total Tasks	3	
Jeng Yue	Readings for IPP Guidelines	1.5	
	Readings for IPP 7 - Unique Identifiers	1.5	
	Readings for IPP 1 - Collection	1.5	
	Report write up	0.5	
	Meetings	1	Report Discussion
	Total Hours	6	
	Total Tasks	5	
Nassar	reading about ipp and app	2	
	investigating the data input for the system	0.5	
	Writing up principles consulted and data type collected section	1.5	
	setting up google docs	0.25	
	formatting the final report	1	
	meeting	1	Report Discussion
	Total Hours	6.25	
	Total Tasks	6	
Wei Han	Meetings	1	Report Discussion
	Readings on IPP and APP	4	
	Write up on summary, introduction and conclusion	2	
	Total Hours	7	
	Total Tasks	3	
Chee Feng	Meetings	1	Report Discussion
	Write report	1.5	
	Reading up IPP guideline	2.5	
	Total Hours	5	
	Total Tasks	3	