TSSM™
Creating VCE Success

Software Development Teach Yourself Series

Topic 10: Legal Obligations Unit 4

A: Level 14, 474 Flinders Street Melbourne VIC 3000
T: 1300 134 518 **W:** tssm.com.au **E:** info@tssm.com.au

Contents

CASE STUDY

All Teach Yourself Series in this package will refer to the following case study.

Tariq Mulner is the manager of a school canteen. He manages how many lunches are going to be prepared each day. It is difficult to tell how many lunches will be sold, so he would like a software solution that students can use to order lunches. This application would provide him with a complete list of orders.
Most of the students have smart phones, so Tariq is suggesting the solution is a phone app that can read in the lunch order, and send it to his device so he can print out the order list.

Photo by Tirachard Kumtanom from Pexels used with permission

Legal Obligations

When software collects and stores sensitive data, the software developer has an obligation to know and adhere to the legislation pertaining to data storage, privacy and ownership.

The Australian and Victorian legislation that relates to software development are:

- The Privacy Act 1988 (and the 13 Privacy Principles)
- The Privacy and Data Protection Act 2014
- The Copyright Act 1968
- The Health Records Act 2001

Privacy

The Privacy Act regulates how personal information is handled. All information related to the individual and their finances, opinions and practices include:

- Name
- Signature
- Address
- Phone number
- Date of birth
- Medical records
- Financial records
- Bank details
- Government records such as driver's license and tax file number

There are 13 Privacy Principles that govern the way all data is handled and need to be kept in mind when developing a software solution that collects user information.

The Australian Privacy Principles (APP) below are outlined as per the Office of the Australian Information Commissioner website: oaic.gov.au/privacy

Principle	**Title**	**Purpose**
APP 1	Open and transparent management of personal information	Organisations must manage personal information in an open and transparent way. This includes having a clearly expressed and up to date privacy policy.
APP 2	Anonymity and pseudonymity	Organisations to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.
APP 3	Collection of solicited personal information	Outlines when an organisation can collect personal information that is solicited. It applies higher standards to the collection of sensitive information.
APP 4	Dealing with unsolicited personal information	Outlines how organisations must deal with unsolicited personal information.

APP 5	Notification of the collection of personal information	Outlines when and in what circumstances an organisation that collects personal information must tell an individual about certain matters.
APP 6	Use or disclosure of personal information	Outlines the circumstances in which an organisation may use or disclose personal information that it holds.
APP 7	Direct marketing	An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.
APP 8	Cross-border disclosure of personal information	Outlines the steps an organisation must take to protect personal information before it is disclosed overseas.
APP 9	Adoption, use or disclosure of government related identifiers	Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual. (Example: driver's license number, tax file number etc)
APP 10	Quality of personal information	An organisation must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An organisation must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.
APP 11	Security of personal information	An organisation must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An organisation has obligations to destroy or de-identify personal information in certain circumstances.
APP 12	Access to personal information	Outlines an organisation's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.
APP 13	Correction of personal information	Outlines an organisation's obligations in relation to correcting the personal information it holds about individuals.

The Canteen Application developed for Tariq will be affected by the Privacy Act. Customers will require accounts that hold their personal details. When developing a system that stores personal information, it will be important for you as the developer to meet the obligations outlined by the Privacy Principles.

APP1: When the user downloads and installs the Canteen App, they must be informed that their data is being stored in a database. User should also be informed that they can request to see their data and how it is used.

APP2: Users may not have the option to not identify themselves –since they must be members of the school community to have the app.

APP3: Collecting data from staff and students are restricted for the purposes relevant to the operation of the app.

APP4: Any unsolicited personal information must be destroyed if not from a member of the school community.

APP5: When personal information such as medical issues (nut allergies) are collected in student records, the users must be informed.

APP6: The data collected from the users cannot be transferred to another organization without first obtaining permission from the students.

APP7: The data collected cannot be used for direct marketing unless permission is provided when the data is provided.

APP8: It is preferred to store data locally rather than in international cloud storage because other organization outside of Australia are not subject to our legislation.

APP9: No government identifiers are required for the Canteen Application – only the school ID.

APP10: The database must be kept up to date. The app could frequently ask if the user data is still correct and give the user the option to update their personal details.

APP11: The server where the personal information must be stored in a locked location. Access should be limited through authentication such as username and password login processes.

APP12: If a user requests access to their information it must be provided.

APP13: A User has the right to have any incorrect data stored in the system corrected.

Privacy and Data Protection

The purpose of the Privacy and Data Protection Act 2014 includes the following:

- to promote awareness and understanding of the Information Privacy Principles (IPPs);
- to receive complaints about possible breaches of the IPPs by the Victorian public sector;
- to conduct audits to assess compliance with the IPPs; and
- to undertake research, issue reports, guidelines and other materials with regard to information privacy.

The Information and Privacy Principles place strict obligations on organizations that collect, store, use and disclose personal information.

Collection of Data

An organisation may request personal information from an individual or from a third party provided the following criteria are met:

- the organisation must only ask for the specific personal information required to fulfil the lawful purpose that is directly related to the function of the organisation
- if the information is collected directly from an individual, the organisation must tell the individual what the information is going to be used for before, or at the point of collection where possible, if not possible – as soon as practicable after the information is collected
- the organisation must not collect information by unlawful or unfair means, including by trickery, deception or misleading conduct.

Storage and Security

Organisations must ensure that documents containing personal information are protected from:

- loss
- unauthorised access, use, modification or disclosure; and
- any other misuse.

The level of storage and security will depend upon the nature of the personal information in the document and the risk of a security breach occurring. If a document contains extremely sensitive

information, such as health or criminal records, an agency should take maximum care in protecting the information.

Access and amendment

Organizations are required to disclose to the public the general types of information they hold, for what particular purpose, and how the information is proposed to be used.

Use and disclosure

Personal information must not be used for a purpose other than the particular purpose for which it was obtained, unless certain exceptions apply. Personal information must not be disclosed to a third party, unless certain exceptions apply. Some of the exceptions include, for example:

- where the individual has expressly or impliedly agreed to the use/disclosure
- where the use/disclosure is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare
- where the use/disclosure is required or authorised under law or necessary for law enforcement purposes; and
- where the use/disclosure is necessary for research or statistical purposes.

Serious breaches of the Privacy Act can attract hefty fines.

Copyright

The Copyright Act 1968 governs the ownership of creative works such as text, photographs, music, computer programs, films, sound recordings and other images. The rights to use the creative works belong to the creator automatically. Copyright owners have the right to prevent others from reproducing or communicating their work without permission.

Software developers need to negotiate the ownership of the solution produced with the client. If a client is paying you to produce a software product exclusively, then they would not want you providing that same solution to other clients.

A common issue in software development is reverse engineering software solutions to produce similar products. The copyright Act protects the author of the original software unless that author has provided the ware under creative commons to the public.

When producing a software solution for Tariq's Canteen, you might be tempted to use functions available on GitHub shared for non-commercial purposes. It is important that you, as a developer, do not breach the copyright of other creator's work when finding solutions to your own software development problems.

Health Records

Health information collected by organisations is subject to the Health Records Act 2001. Health information includes:

- physical or mental health, or disability of an individual,
- expressed preferences for future provision of health care,
- the nature of health care provided to an individual,
- information collected in the course of provided health care,
- information collected in connection to the donation of human tissue,
- genetic information that could be predictive of an individual's health.

Organizations subject to the Health Records Act are:

- Victoria government organisations and public bodies,
- Universities, schools and other education or child-based organisations,
- Researchers,
- Blood and tissue banks,
- Public and private employers in relation to their employee personnel records,
- Counsellors,
- Insurance and superannuation organisations,
- Gymnasiums,
- Other organisations that hold health information.

Schools collect health records for distribution among staff in an effort to ensure that if an emergency occurs, staff will be able to respond according to the child's needs. It is possible, with the growing number of students suffering food allergies, this data may be requested to be incorporated in the Canteen Application. A Code of Conduct may be required for data access and use for Canteen staff.

Review Questions

Applied Questions

Tariq has asked you to produce an app. The Analysis is available in TOPIC 1. You have 3 weeks to develop the app to hand over. Ideally Tariq should have the solution for 2 weeks before evaluation begins.

1. Why should Tariq use a local server rather than a cheaper data storage cloud service based in the U.S?

A. A local server would be faster and he is legally obliged to ensure a fast connection to the data.

B. Keeping data in Australia ensures the security for the data is governed by protective legislation.

C. It is easier to manage back-ups locally that across the internet.

2. Why must software developers be familiar with the Privacy Act?

A. So they can develop a code of conduct for the organization in management of data.

B. To ensure they do not use the data for anything other than its intended purpose

C. To ensure the data is secure and measures are implemented so it can be updated.

3. Copyright is:

A. The exclusive right to use a creative work.

B. Ownership of a creative work.

C. Both A and B.

4. A Melbourne nightclub ran a competition offering free drinks to customers who responded to social media post with their phone number. The nightclub used the phone numbers to contact the customers about other events without informing them they would use their numbers for that purpose. Which APP is relevant to this breach of privacy legislation?

A. APP7

B. APP9

C. APP11

5. Why would most organisations require an understanding of the Health Records Act and ensure provisions to protect data related under the Act?

Solutions to Review Questions

1. B. Keeping data in Australia ensures the security for the data is governed by protective legislation.

2. C. To ensure the data is secure and measures are implemented so it can be updated.

3. C. Both A and B.

4. A. APP7

5. Most organizations are employers and human resources often keep any data on employee health issues on record.