Workplace Information Handling Workbook

Scenario:

You are working for the independent game studio *Derivative Games* and are on the planning team for their new game *Diavolo 3*.

Although the studio is profitable this will be the largest project they have released. Management expects sales of the game to increase the company’s annual turnover to over $3 million.

The owner and founder would like to use the existing customer database to send marketing material directly to customers via email. This has raised some concern amongst the team as the company does not have an existing ‘opt-in’ mailing list (although it does have customer email addresses stored in their customer database), or a policy on direct marketing.

The company would also like to start taking pre-orders for the game once development has reached the *beta* milestone, which is scheduled for 3 months from now. This will require the collection of personal information and payment from customers. You will need to ensure that this information is stored securely so that all customers receive their orders once the game is released.

You have found the existing privacy policy for *Derivative Games*, but you’re not sure if this adequately informs customers of how their data is used, or if it will cover how your team would like to use customers’ personal information for this project.

With reference to the scenario above, answer the following questions (answer in the boxes provided):

Question 1:

In Australia, what piece of legislation regulates the way individuals’ personal information is handled?

|  |
| --- |
| Privacy Act 1988 |

Question 2:

Within the legislation from Question 1, there are 13 principles. Collectively, what are these principles called?

|  |
| --- |
| Australian Privacy Principle 1—open and transparent management of personal information  Australian Privacy Principle 2—anonymity and pseudonymity  Australian Privacy Principle 3—collection of solicited personal information  Australian Privacy Principle 4—dealing with unsolicited personal information  Australian Privacy Principle 5—notification of the collection of personal information  Australian Privacy Principle 6—use or disclosure of personal information  Australian Privacy Principle 7—direct marketing  Australian Privacy Principle 8—cross‑border disclosure of personal information  Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers  Australian Privacy Principle 10—quality of personal information  Australian Privacy Principle 11—security of personal information  Australian Privacy Principle 12—access to personal information  Australian Privacy Principle 13—correction of personal information |

Question 3:

Based on the information you have, will *Derivative Games* need to comply with this legislation? Why?

|  |
| --- |
| Yes, as Derivative Games will turnover more than $3 million a year and hence has to follow the 13 privacy policies listed above. |

Question 4:

For the purposes of this project, we will classify workplace data using three types: non-sensitive data, proprietary information, and personal information.

*Proprietary information*: information that the company wishes to keep secret. This may include business strategy, employment contracts, game designs, source code, and similar information.

*Personal information*: any personally identifiable information, whether this belongs to customers, business partners and contractors, or direct employees.

*Non-sensitive information*: publicly available data and other data not included in the definition of personal information or proprietary information.

Identify as many types of workplace data as you can from the scenario and classify them according to these three data types. (You may speculate about the information various teams within the company may need to work with for the project described in the scenario – for example, the source code the developers work on for *Diavolo 3* would be classified as proprietary information).

Try to list 2 pieces of information for each type. You may wish to discuss this with your group or class.

|  |  |  |
| --- | --- | --- |
| Non-Sensitive Information | Proprietary Information | Personal Information |
| Made by Derivative games  Title of the games | - project source code  Contracts with the publisher  Employment contracts | User account details  Credit information  TFN, address both users and employees |

Question 5:

List all personally identifiable information that you think *Derivative Games* will need to collect for this project . (Aim for at least 2 items. The first one has been provided for you)

As you list each piece of PII, consider whether it is actually necessary to collect and hold that personal information in order to carry out your functions and activities. (Over-collection can increase risks for the security of personal information).

|  |  |
| --- | --- |
| Business Use | Personal Information Collected |
| e-mail mailing list | e-mail address |
| Pre-Orders | Name, Payment Method, Billing Address |
| Beta Testers | Player Account ID |
| Marketing and advertisements | Update privacy policy and opt out method |
|  |  |
|  |  |

Question 6:

For each piece of personal information collected, plan how the personal information will be handled.

List how the personal information will be stored and who will have access to it.

Consider how privacy protections can be embedded into the handling process, or how existing privacy protections could be strengthened.

You may wish to discuss this question with your team or class.

|  |  |
| --- | --- |
| PII Collected | Handling Process |
| e-mail address | e-mail addresses collected via web form and automatically stored in a company owned database Access to the database can be controlled with a password |
| Payment Method | Collected via player’s buying the game, automatically stored in a secure data base that is password protected and encrypted, only accessible from a few select individuals. |
| Player Account ID | Collected via player signing up for beta testing, automatically stored in a company database regulated with a password and only accessible to select individuals. |
|  |  |
|  |  |
|  |  |

Question 7:

Review *Derivative Game’s* privacy policy.

In your opinion, does the existing policy adequately inform customers about how their personal information could be used?

|  |
| --- |
| No, not entirely, as it is there are several things left out. |

If no, identify the areas where the policy would need to be modified. You may wish to discuss this with your team or class.

|  |
| --- |
| As it is there is no mention of the use of private information for marketing purposes, and there is no visible opt-out option which would be necessary to be added and updated in the privacy policy before any of the personal information can be used for marketing.  The policy would have to cover the organisations opt out policy and to provide the user, on request, the source for the individual’s private information, and a way to change any out dated information that may have been collected. |

Question 8:

Your team is considering using an external marketing company, *Helping You*, to conduct marketing activities on behalf of *Derivative Games*. *Derivative Games* would need to give *Helping You* access to some personal information of customers, like names and email addresses. This company is based the US.

Which of the 13 principles from Question 2 would *Derivative Games* need to consider, and why?

|  |
| --- |
| APP 1: Transparent on how customer data is used  APP 5: Inform whether the personal information disclosed to overseas participants  APP 6: Personal information can only be used or disclosed for what is was originally disclosed for, unless otherwise permitted by the customer.  APP 8: Inform of cross boarder disclosure of personal information |

Question 9:

Review the lesson on *Data Integrity Threats*.

What are three common threats to data integrity?

|  |
| --- |
| Inadequate Back-up and Recovery |
| Improper Security Networks |
| Poor Passwords |

|  |
| --- |
| Ensure strong passwords are used, secondary verification, through a link sent to an email or phone number associated with the account.  Avoid using public networks or unconfirmed and unknown networks that may not be secure.  Ensure Passwords or other data is kept in a secured location, that has back ups and isn’t just a single copy that could be subject to loss, damage or corruption. |

What are some ways the company could minimise these threats?