Policy: Information Privacy Guideline

Corporate Services, Corporate & Franchisee

THE COFFEE CLUB

Information Table

Date	31 December 2020
Person Responsible	Brad Dight – Head of Technology
Department	Technology

Policy: Information Privacy Guideline

1. Summary

This Policy reflects Minor DKL Food Group's (**Minor DKL**) obligations in managing personal information as regulated by the *Privacy Act 1988* (Cth) (**Privacy Act**) and *Information Privacy Act 2009* (Qld) (**the IP Act**).

The object of both Acts is to provide for the fair collection and handling of personal information and a right of access to and amendment of personal information held or controlled by Minor DKL.

2. What information is covered by this Policy?

This Policy applies to:

- personal information collected by Minor DKL for inclusion in a document or generally available publication, or contained in a document held or controlled by Minor DKL; and

- the activities of Minor DKL employees, contractors, consultants and agents (defined as Minor DKL Officers in this guideline).

3. Who is responsible under this Policy?

All Minor DKL Employees have the accountability to ensure that the personal information they handle in their everyday duties is managed in accordance with the Acts.

Each department is responsible for ensuring appropriate privacy procedures are in place for their group.

4. What are Minor DKL's obligations?

What are Minor DKL's privacy obligations?

A summary of Minor DKL key privacy obligations regarding the collection, storage, use and disclosure of personal information is set out in the Policy: Notifiable Data Breaches.

What are Minor DKL privacy obligations regarding contractors?

If Minor DKL engages an external party (contracted service provider) to perform some of its functions or activities, and the engagement involves the handling of personal information, Minor DKL must take all reasonable steps to bind the provider to comply with the Acts.

What activities could involve privacy issues?

Minor DKL Employees deal with personal information when undertaking most of their duties, including but not limited to:

- Media enquiries;
- Incoming correspondence from the public or other agencies;
- Handling personnel issues and recruitment;
- Processing an application or membership;
- Using or designing forms, processes or systems to collect information from the public (competitions); and
- Handling complaints

What is personal information?

Personal information is any information or opinion that may lead to the identity of a person.

For information to be personal information:

- it must be about the individual;
- the individual's identity must be apparent or reasonably ascertainable from the information; and
- it can be true or not.

Examples of personal information include, but are not limited to:

- Individual's name (including previous names);
- Date of birth;
- Marital status;
- Individual's photo;
- Individual's work details (including phone number and email address);

- Individual's likes or opinions;
- Individual's health, criminal, payroll and financial information;
- Information that a person has not paid a debt or fine;
- A person's comments on another's aptitude and performance.

What is a document containing personal information?

Personal information may be in any material or digital form, including but not limited to:

- Correspondence;
- Emails;
- Instant messages;
- Database;
- Audio recordings;
- Image/photos;
- Job applications.

Minor DKL's collection obligations

When do I need to provide a collection notice?

A collection notice is a statement required to be given to an individual:

- whenever Minor DKL collects personal information directly from the individual it is about (i.e. solicited information); and

- if the information will be included in a document or a generally available publication.

When is a collection notice given?

Minor DKL should provide the collection notice before, or at the same time as, the information is collected.

What do I need to include in a collection notice?

Minor DKL must take all reasonable steps to make an individual generally aware of:

- why the information is being collected – the explanation needs to be more than a general reference to a broad function;

- any law that allows or requires the collection – and, if so, which law; and

- any entity to whom Minor DKL may give the information and, if known, anyone who they will in turn give the information.

How can I give a collection notice?

There is no prescribed means to give a collection notice. Some examples include:

- A written notice which is readily accessible on Minor DKL's website.
- A written statement in a form or in a leaflet sent with other correspondence.
- A written statement made available through signage.
- A verbal notice which is made available as a recorded option for incoming telephone calls, or set out in a script which is read out to individuals by staff.

An example of a collection notice is as follows:

Minor DKL Food Group is collecting the information on this form for the purposes of [insert a statement of purpose]. This information is [authorised/required] by [insert name of Act or regulation, if any]. Minor DKL Food Group usually gives some of or all this information to [list names of recipient organisations, or if shorter organisation types]. Your personal information will not be disclosed to any third party without your consent unless authorised or required to do so by law.

How do I handle unsolicited personal information?

Unsolicited personal information is information that Minor DKL receives but has taken no active steps to collect.

Minor DKL may receive unsolicited personal information when:

- Minor DKL requests specific personal information and the individual provides more information than has been requested; and
- An individual sends personal information to Minor DKL that it has not asked for.

Examples include where:

- Employment application sent to Minor DKL that is not in response to an advertised vacancy;
- Documents provided with an application form which were not requested;

- Unsolicited correspondence sent to Minor DKL;
- Email that is accidentally copied to a Minor DKL Employee;
- Promotional flyer containing personal information promoting the individual's business or services.

No collection notice is required to be given where Minor DKL receives unsolicited personal information. However, Minor DKL must still comply with its other privacy obligations under the IP Act in relation to the information, including:

- collecting the information lawfully and fairly;
- storing the information securely; and
- limited and careful use and disclosure of the information.

5. Use of Personal Information

For what purpose may Minor DKL use personal information?

Minor DKL may only use personal information for the purpose for which it was obtained, unless:

- the secondary purpose is directly related to the primary purpose;
- the individual has expressly or impliedly agreed to the use for the secondary purpose;
- the use 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;
- the use is authorised or required under law;
- the use is necessary for law enforcement purposes; or
- the use is necessary for research or statistical purposes.

What personal information may be used by Minor DKL?

Minor DKL may only use those parts of the personal information which are directly relevant to fulfilling the purpose for which it was collected, unless otherwise permitted by the IP Act.

6. Disclosure of Personal Information

When can Minor DKL disclose information to a third party?

Minor DKL Officers must not disclose personal information to a third party, unless:

- the individual is reasonably likely to be aware that it is the agency's usual practice to disclose that type of personal information to the third party;
- the individual has expressly or impliedly agreed to the disclosure;
- the 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;
- the disclosure is authorised or required under law;
- the disclosure is necessary for law enforcement purposes;
- the Australian Security Intelligence Organisation (ASIO) has asked Minor DKL to disclose the information; or
- the disclosure is necessary for research or statistical purposes.

What can Minor DKL disclose to a third party?

Minor DKL may only disclose those parts of the personal information which are directly relevant to fulfilling the purpose for which it was collected, unless otherwise permitted by the IP Act.

Keep in mind:

- sharing only what is reasonable and necessary; and
- whether the objective can be achieved without sharing the personal information (e.g. redaction of name and contact details).

When can Minor DKL disclose routine personal information to a third party?

Routine personal work information may be disclosed in most circumstances if there is an appropriate basis to expect there would be no prejudice to a person's privacy or cause of public interest harm.

Examples include:

- Work email address or phone number;
- Job title;

- Work classification;
- A professional opinion given wholly in a professional capacity.

7. Handling Requests and Complaints

What happens if a potential privacy breach has been identified?

Please notify the Privacy Officer of any potential privacy breach.

What is the Notifiable Data Breach (NDB) Scheme and how does it affect Minor DKL?

Please refer to the Policy on Notifiable Data Breaches.

The NDB scheme requires entities to report to the subject individual and the Australian Information Commission regarding privacy breaches that are likely to result in serious harm to an individual.

The scope of the NDB provisions are very broad and may include something as simple as a Minor DKL staff member losing a laptop that allows access to sensitive information or a more extreme example of an external party "hacking" an online Minor DKL system.

Any potential breach involving sensitive information must be immediately notified to the privacy Officer (privacy@minordkl.com.au)

What to do if a person requests access to or amendment of personal information held by Minor DKL?

Please refer any request for access or amendment to the Privacy Contact Officer.

What to do if a person makes a privacy complaint?

A privacy complaint may be made by an individual about Minor DKL's handling of that individual's personal information.

When is a privacy complaint handled by the Privacy Commissioner?

If the complaint is not resolved by Minor DKL through its internal processes and at least 45 business days have elapsed since the complaint was made to Minor DKL, that person may refer his or her complaint to the Privacy Commissioner.

Ultimately, if the complainant is not satisfied with the Privacy Commissioner's

decision, or the complaint is not resolved by mediation between the complainant and Minor DKL (via the Privacy Commissioner), the matter may be referred to the Queensland Civil and Administrative Tribunal (QCAT).

QCAT may make appropriate orders including payment of compensation to the individual of up to $100,000.

8. Privacy Impact Assessment (PIA) Process

What is a PIA?

A PIA is a tool that agencies can use to assess the privacy impacts of a new project and where necessary, identify ways in which the obligations set out in the IP Act can be met. Conducting a PIA is not mandatory under the IP Act however the OIC strongly encourages the use of PIAs as part of taking a 'privacy by design' approach, and making privacy a key consideration in the early stages of a project and throughout its lifecycle.

The full process for preparing a PIA is outlined in the OIC's Guideline: Undertaking a Privacy Impact Assessment (PIA Guideline), which is available on the OIC website, along with supporting resources, such as the threshold privacy assessment tool and PIA report template.

Overview of a PIA

A PIA process would be undertaken for any project, initiative or system that may involve the handling of personal information. While each project is different, a PIA should generally include the following steps:

1. Conduct a threshold assessment	Determine whether a PIA is needed. A PIA is beneficial for projects that will deliver a new or changed way of handling personal information. Use the OIC threshold privacy assessment tool if you are unsure whether to conduct a PIA.
2. Plan the PIA	Consider who will conduct the PIA and how detailed it needs to be. When will it need to be delivered? Who are the internal and external stakeholders and what amount and timing of consultation will be needed?
3. Describe the project	Document what the project will deliver and what it will achieve, why it is needed, and whether it is part of a larger program. A PIA report template is available for you to capture information gathered throughout the PIA process.

4. Identify and consult with stakeholders	Identify who is affected by or has an interest in the project, how extensive the consultation needs to be and how and when the consultation will be undertaken. Consultation may need to occur throughout the PIA process rather than at a single point.
5. Map the personal information flow	Describe what personal information will be involved and how it will be collected, used and disclosed, including how it will be stored and protected. Consider using a diagram or table to set out the key information for the different types of personal information involved in the project.
6. Identify the privacy impacts	Analyse the projects personal information handling practices against the privacy obligations set out in the IP Act to identify any privacy impacts. The PIA report template has questions to help you identify potential privacy impacts. Your analysis should also include any stakeholder consultation results.
7. Identify options to address privacy impacts	Consider what options will address the privacy impacts. If there are multiple options, evaluate the cost, risk and benefit of each option to identify the most appropriate one. Options may include operational controls (such as training), technical controls (such as passwords) and communication strategies.
8. Produce a PIA report	Prepare a report for approval by the Project Executive, Steering Committee or senior management. Publishing a PIA report can demonstrate a commitment to the openness and transparency and show that the project has been designed with privacy in mind.
9. Respond and review	Take action to implement the agreed recommendations, either by preparing an implementation plan or by integrating the agreed actions into the project plan. A PIA is a living document. It should be updated as changes are made to the design or implementation of the project.

9. Contact

If you have any queries with respect to this policy, please contact: support@minordkl.com.au or privacy@minordkl.com.au.

For more information, please see:

- Data Breach Preparation & Response Guide
- Australian Information Commissioner's role in the NDB scheme
- Guide to OAIC privacy regulatory action — Data breach incidents