Digital Technologies Geelong

PRIVACY AND DATA PROTECTION PROCEDURE

Enacting the requirements of the Information Privacy Principles (IPPs) under the *Privacy and Data Protection Act* 2014

Where required, relevant personnel at Digital Technologies Geelong will enact the requirements of the Information Privacy Principles (IPPs) listed in this table.	
Information Privacy Principles	Responsibility
IPP 1 – Collection Only collection personal information that is necessary for the purpose, function and performance of OCS and relevant entities. Ensure individuals we collect information from are able to gain access to their data and that they are informed of the following: • The primary purpose for collecting the information • Which entities the information may be disclosed to • Their right to access and correct any information • Whether or not their information will be stored with a third-party provider • How to directly access or request access to their personal information	All staff who collect personal information
IPP 2 – Use and disclosure Personal information should only be used for the purpose it was originally collected, with any secondary uses being for purposes the person would reasonably expect, with their consent. Exceptions are as follows: • The secondary purpose for use and disclosure is related to the primary purpose and a person would reasonably expect this • Where the information is lawfully requested in the interests of law enforcement, individual health and safety and welfare, or other legislative requirements	All staff with access to personal information
IPP 3 – Data quality Ensure that personal information DTG collects is accurate, complete and up-to-date.	All staff managing personal information

IPP 4 – Data security Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. DTG will take reasonable steps to destroy or de-identify information that is no longer needed for its primary or secondary purposes. All staff must take reasonable steps to protect the personal information collected, stored and used by DTG.	All staff with access to personal information
IPP 5 – Openness Make clear the policies and procedures on how personal information is handled by making all relevant documents internally and available on the DTG website.	Nominated staff
IPP 6 – Access ad correction Ensure individuals are able to access the personal information DTG collections and make amendments and corrections. Access may also be managed under the *Victorian Freedom of Information Act* 1982. DTG is to correct information where a written request is received (except where legislation forbids it): • For staff information • For client information DTG should not provide access to or corrections of information under the following circumstances if: • Providing access to the information would pose a serious and imminent threat to the life and health of any individual • Providing access would have an unreasonable impact on the privacy of individuals • Providing access would be unlawful or be likely to enable unlawful activity	All staff collecting and managing personal information
IPP 7 – Unique identifiers Unique identifiers, such as Tax File Numbers and Driver's License Numbers allow data to be matched with individuals. Where possible, DTG staff should avoid collecting and sharing unique identifiers.	All staff collecting and managing personal information
IPP 8 – Anonymity Individuals whose data is collection should have the option of not identifying themselves, within what legislation permits.	All staff
IPP 9 – Trans border data flows The purpose and function of DTG requires that personal data be sometimes transferred to third parties. In these occurrences the standards of privacy and data security should travel with it. DTG should only transfer data to	All staff handling personal information in this context

third parties if it can verify that their privacy and security standards are similar or equal to those set out under the Victorian Information Privacy Principles.	
IPP 10 – Sensitive information Legislation prohibits the collection of sensitive information such as racial origin, political views, religious beliefs, sexual preferences, membership of political, professional or industrial groups, or criminal record. DTG will only collect sensitive information under certain circumstances, as outlined in the *Privacy and Data Protection Act 2014.* These circumstances include: • Where the person consents to the information being collected • Where the collection of sensitive information is required by law • Where the collection is necessary to protect the safety and lives of an individual or individuals • Where there is government funded research and no other means of information collection is practicable to obtain that information, *and* where obtaining consent is not practical.	All staff handling personal information in this context

Health Information

In some circumstances it is necessary for DTG to collect and handle health information from its employees and contractors. This information may include declared disabilities, chronic illnesses or other underlying health issues, and other information relevant to maintaining safe working conditions.

All requests for an individual to access their own personal health information must be made in writing.

Access to others' personal health information is strictly prohibited except in circumstances where:

- The information is being used for its primary purpose of maintaining safe working conditions
- The information is being updated by the individual in question and administrative staff are required to make those changes
- The information is initially being collected and stored, typically as part of the hiring process at DTG

Other privacy requirements

Images

Use of any person featured in any image (photo or video) requires written and signed consent to use the image by the person in question. As long as the image(s) are used, consent must be maintained. Where consent is not practical (e.g. the filming of crowds during events or company tours), signs must be posted to alert attendees that images are being taken.

Documents

All documents intended for or otherwise requiring the collection of personal information should have relevant notices included within the document.

Non-compliance and disciplinary actions

It is the responsibility of Digital Technologies Geelong to provide a consistent and fair procedure for any complaints relating to privacy and personal information. This procedure applies if any individual believes that DTG has acted in a manner that has breached a Privacy Principle.

All staff are required to take reasonable steps to meet the requirements of the Privacy and Data Security Procedure and Policy, to ensure that their own and others' privacy rights are maintained. Third party contractors are also required to take reasonable steps to meet these requirements.

Making a complaint

Complaints can be directed to the DTG Privacy Officer.

Privacy@orionconsumerservices.com.au

Privacy Officer

Digital Technologies Geelong Branch

Boundary Rd

Thomson Victoria

Alternatively, a person may contact the Privacy and Data Protection Commissioner.

privacy@cpdp.vic.gov.au

Commissioner for Privacy and Data Protection

PO Box 24014

Melbourne

Victoria 3001

Phone: 1300 666 444

Process for managing a complaint

Complaints must be forwarded to the General Counsel and Company Secretary within six months of the complainant becoming aware of the initial issue. The complaint must specify the details of the issue.

Incident response and management

An incident (or data breach) occurs when information held by DTG is lost, or is accessed, modified, disclosed or otherwise misused by an unauthorised party. The DTG response plan is as follows:

1. Contain the breach (stop the practice, shut down the system involved, recover the records)
2. Evaluate the risks
    a. Record the time and date of discovering the suspected breach, staff or other personnel involved, cause of the breach, extent of damage, and overview of content affected
    b. Ensure any evidence related to the incident is safely maintained
    c. Assess the situation based on what is known so far about the incident
3. Notify relevant parties
    a. Immediately notify manager. Manager to immediately notify director.
    b. Immediately notify Privacy Officer.
    c. Determine who else needs to be made aware of the incident
    d. Before notifying affected individuals, determine if there is any risk of harm to the individuals
    e. Determine whether other organisations, such as law enforcement, should be notified
4. Rectify cause of incident
    a. Complete a full investigation of the incident
    b. Update policy and procedures if necessary
    c. Assess whether staff training practices need improvement and update if necessary
    d. Update security response plan in accordance with outcome of investigation

Collection, access to and storage of information

Collection and storage of sensitive information is the responsibility of the DTG Data Services in compliance with their work practice, in accordance with DTG policy and procedure.

- Any employee wishing to access their personal information for any purpose must submit a request in writing to DTG Data Services.
- Any employee wishing to correct information must submit a written request to DTG Data Services.
- DTG Data Services is required to respond with a decision to any such requests within 30 days.
- Any request from parties external to DTG must be forwarded to the Privacy Officer to confirm the legality of the request.

Review

This procedure must be reviewed no later than four (4) years from the date of approval. The policy and associated procedures will remain in force until such time as they have been reviewed and re-approved or rescinded. The policy and procedures may be rescinded or amended as part of continuous improvement prior to the scheduled review date.

Further information

Approval Body	Digital Technologies Geelong Board of Directors
Date approved	14/09/2013
Document ID	PPDDV05
Owner	Martha Geoghan
Author	Andrew Wright
Amendment	12/10/2017

Original source: https://www.datocms-assets.com/6783/1613605939-prolr04-privacy-data-protection-procedure-v2-2016-amended-8-april-2019.pdf