POLICY AND PROCEDURE

Policy Name:	**Privacy**
Section:	General
Approved By:	E-focus CEO 2018
Last Reviewed:	February 2018

SECTION 1 – INTRODUCTION

PURPOSE

To establish organisational guidelines which must be observed by all employees to protect employee, and client privacy and confidentiality.

To outline the minimum standards of conduct overarching for the organisation related to the policy topic. This policy is complimentary to specific standards and codes outlined in the organisation's underpinning Government contracts / agreements.

PRINCIPLES

This policy is guided by the legislation and principles of protecting the privacy of clients, employees and the organisation, and compliance with privacy laws and standards. (see attached short version of Privacy Principles) and link to Notifiable Data Breaches (NDB) scheme.

SCOPE

This policy and procedure applies to E-focus ("the organisation") and subsidiaries and activities

EXCLUSIONS

Nil

LEGISLATIVE CONTEXT

Information Privacy Act (Vic.) 2000
Privacy Act (Commonwealth) 1988
Health Records Act (Vic.) 2001
Freedom of Information Act (Vic.) 1982
Public Records Act (Vic.) 1973.
National Privacy Principles
Notifiable Data Breaches (NDB) scheme

DEFINITIONS

Word / Term	Definition
Personal Information	Is information or an opinion that identifies an individual or allows their identity to be readily worked out from the information. It includes information such as a person's name, address, financial information, marital status or billing details
Sensitive Information	Is a subset of personal information. It includes information about a person's racial or ethic origin, political opinion or membership, religious beliefs or affiliations, sexual preferences, criminal records or health records. A higher level of privacy protection applies to sensitive information.
Health Information	Means personal information about an individual that includes (a) Information or opinion about – i. The physical, mental or psychological health (at any time) of an individual; or ii. A disability (at any time) of an individual
Record	Includes information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not (eg hard copy, audio tapes, photographs, micro-fiche and computerised records including electronically derived databases and directories), about a person whose identity is apparent, or can reasonably ascertained, from the information or opinion.
Primary Purpose	A primary purpose is one for which the individual concerned would expect their information to be used. Using the information for this purpose would be within their reasonable expectations.
Secondary Purpose	A secondary purpose may or may not be apparent to the individual concerned, or within their reasonable expectations. Collecting information may be mandatory (because required by law) or optional. The main distinction is that the service could still be provided even if the secondary purpose were not serviced.
Privacy Statement	A statement related to the privacy of personal information which appears on all documents and forms generated by the organisation and used for the collection of information, and that is appropriate to the information being collected. This excludes documents used by the organisation to collect information which are generated by Government departments and used under contractual obligation.
Notifiable Data Breaches (NDB)	The NDB sets out the requirements and process for notifying and reporting an eligible data breach. Information attached to this policy refers to online resources and the role of Office of Australian Information Commission (OAIC)

SECTION 2 – POLICY

1. Collection of Information

The organisation will only collect personal information about a person if it is necessary for one or more of its functions or activities. At the time of collection, the organisation will explain to the person the purpose, proposed use, disclosure and rights of access.

Information (personal and sensitive) will only be collected with the consent of the individual. Personal information from a person or legally authorised representative will be required in accordance with contractual and legislative requirements.

2. Use and Disclosure

Personal information is used and disclosed only for the purposes for which it was collected and is protected from misuse. Personal information can be shared if:

- It is necessary for the purpose it was collected, or a secondary purpose directly related to that purpose;
- The person consents to the discloser of their information, or the disclosure is necessary to lessen/prevent a serious and imminent threat to life, health or safety;
- The disclosure is authorised by law, or for law enforcement or investigation.

3. Data Quality

The organisation will ensure that all personal information collected, used or disclosed is accurate, complete and up to date.

4. Data Security

All personal information collected is protected from misuse or loss and from unauthorised access, modification or disclosure. Information stored electronically is kept on a secure server and access is restricted to authorised employees. Paper based documents containing personal information are stored securely. Where documents are required to be transferred to another location, personal information is transported securely in an envelope, folder or document bag. Reasonable steps will be taken to destroy or permanently de-identify personal information when it is no longer required for any purpose.

5. Openness

Access to the Privacy Policy and Procedures will be granted to any person making a request for it. On request, all reasonable steps will be taken to inform individuals of the sort of personal information held, its purpose, how it is collected and stored. Information held by the organisation may be accessed by individuals if requested, subject to the requirements of any contractual or legislative requirements.

6. Access & Correction

Access to information by an individual held on that particular individual will be granted should it be requested. If this information is deemed inaccurate by the individual, and this is established, the organisation will take the appropriate steps to correct the information so that it is accurate, complete and up to date.

7. Anonymity

Where lawful and practicable, individuals have the option of not identifying themselves when entering in to transactions with the organisation.

8. Direct Marketing

The personal information collected by the organisation may be used to send individuals direct marketing communication. Sensitive information will not be used for this purpose. Individuals have the option of opting out of direct marketing communications by contacting the Privacy Officer and where practicable, this will be noted on the information being sent.

SECTION 3 – PROCEDURE

	Procedure Steps	Responsibility
1.	**Access to Personal Information**	
	1.1 Access to Personal Information Access to personal information will only be provided under: **1.1(a)** Freedom of Information legislation **1.1(a)** Legislative Obligations **1.1(a)** Individual Consent Arrangements	Staff
	1.2 Access to Personal Information – Staff **1.2(a)** Staff will only be provided with access to personal information where it is necessary to carry out their responsibilities. **1.2(a)** Managers are required to maintain a register of staff who are given access to personal information collected by the division, and whether the staff member may amend or delete the information.	Managers
	1.3 Access to Employee Records Staff may request access to their employee records from: **1.3(a)** Human Resources Manager, for records held by the Human Resources and Finance. **1.3(a)** Site / Manager, for locally held records	CEO, Human Resources / Managers
2.	**Disclosure of Personal Information**	
	2.1 The disclosure of all personal, health and sensitive information is subject to other legislative requirements (eg: The Freedom of Information Act 1982 (Vic.))	Staff
	2.2 The organisation will disclose personal information to a third party on request of an individual, where it receives a written authorisation (Signed) by the individual to be released for a specified purpose. The Manager must co-sign the consent as verification that the individual has properly consented.	Managers
	2.3 The organisation will not require the written authorisation where the disclosure is authorised by law.	

3.	**Privacy Risk Management Procedures**	
	3.1 All Managers have the primary responsibility for privacy compliance in their division. **3.2** Managers must ensure that an appropriate Privacy Statement is in place where their division collects any personal information. These will be developed, where necessary, in consultation with the Privacy Officer. **3.3** Where a Manager is responsible for an information technology system, they are required to ensure that the applicable system complies with privacy legislation. **3.4** The organisation must not acquire or implement information systems that are not privacy compliant.	Managers
4.	**Privacy Complaints Handling Procedure**	
	The following procedure applies if an individual considers that this policy has been breached, or the privacy laws in respect to that individual. **4.1 Complainant to Provide Details of Complaint in Writing** A written complaint must be forwarded to the Privacy Officer within six (6) months of the time the complainant first became aware of the apparent breach. The complaint must specify details of the apparent breach in writing. **4.2 Timeframe for Internal Resolution** Unless principles of due and fair process dictate otherwise, the Privacy Officer must make a determination on a complaint / request to access information within forty-five (45) days of receipt of the complaint, and advise the complainant in writing. **4.3 Response to Complaint** If the Privacy Officer determines that there has been a breach of the policy, he or she will, upon notification of the determination to the complainant, advise relevant personnel in writing and any action required in order to remedy the breach. If the breach is capable of being rectified and is not rectified within thirty (30) days of the advice from the Privacy Officer, the Privacy Officer must inform the CEO. **4.4 Consequences if this Policy is Breached** Disciplinary action may be instigated against any staff member who breaches this policy, which may result in the employee being summarily dismissed in circumstances that the organisation considers there to have been a serious beach. **4.5 Any data breach** Any data breach or breach of the National Privacy Principles will be reported to the CEO and will be managed according to the NDB requirements	Complainant Privacy Officer – CEO Human Resources https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

Regulatory Guidelines

Name	Location
Privacy Statement	
Guidelines to the Information Privacy Principles (issued by Privacy Victoria)	http://www.privacy.vic.gov.au
Guidelines to the National Privacy Principles	http://www.privacy.gov.au/act/guidelines/index.html
Guidelines to Privacy in the Business, Health Sector [under s.95A of the Privacy Act 1988] and Government	http://privacy.gov.au/health/guidelines
Notifiable Data Breaches Scheme	https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme
Office of the Australian Information Commission (OAIC)	https://www.oaic.gov.au/

Submitted Date: 21/02/2018
Approved Date: 21/02/2018
Review Date: 01/01/2020

Commissioner for Privacy and Data Protection

Information sheet

Short guide to the Information Privacy Principles

The ten Information Privacy Principles (IPPs) are contained in Schedule 1 to the *Privacy and Data Protection Act 2014* (PDPA). With limited exemptions, all Victorian Government organisations, contracted service providers and local councils must comply with these principles. This is a short summary of the IPPs. It is intended to provide a high level guide only. For any detailed privacy analysis, please refer to the full text of the IPPs in Schedule 1 of the PDPA.

1 Collection	An organisation can only collect your personal information if it is necessary to fulfill its functions. It must collect information only by lawful and fair means and not in an unreasonably intrusive way. It must provide you notice of the collection, including such things as the purpose of collection and how you can access the information. This is usually done through provision of a Collection Notice that is consistent with an organisation's Privacy Policy. More information on these two documents is available on www.cpdp.vic.gov.au.
2 Use and Disclosure	Your personal information can only be used and disclosed for the primary purpose for which it was collected, for a secondary purpose that you would reasonably expect or in other limited circumstances. It is best that the organisation gets your consent, but the law allows some uses without consent, such as law enforcement purposes and to protect safety.
3 Data Quality	Organisations must keep your personal information accurate, complete and up to date.
4 Data Security	Your personal information must be protected from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify your personal information when it is no longer needed.
5 Openness	Organisations must have clearly expressed policies on the way they manage personal information. You can ask to view an organisation's Privacy Policy.
6 Access and Correction	You have a right to seek access to your own personal information and to make corrections if necessary. An organisation may only refuse in limited circumstances that are detailed in the PDPA, for example where disclosure might threaten someone's safety.
7 Unique Identifiers	Unique identifiers, usually a number, can facilitate data matching. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently by organisations. There are also restrictions that are detailed in the PDPA, on how organisations use unique identifiers assigned by other organisations.
8 Anonymity	Where lawful and feasible, you should have the option of transacting with an organisation without identifying yourself.
9 Transborder Data Flows	If your personal information travels outside Victoria, your privacy protection should travel with it.
10 Sensitive Information	This includes your racial or ethnic origin, political opinions and membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record. The law puts special restrictions on its collection.

Australian Government
Department of Jobs and Small Business

Notifiable Data Breaches Scheme

Obligations of employment service providers

Overview

Employment services providers, and other entities subject to the requirements of the *Privacy Act 1988,* have new obligations under the Notifiable Data Breaches (NDB) scheme for the management of privacy breaches involving personal information, commencing from 22 February 2018.

The NDB scheme requires that any unauthorised access to or disclosure of personal information be assessed to determine whether an 'eligible data breach' has occurred. If so, prompt and appropriate actions must be undertaken. This includes limiting the access and dissemination of the personal information and notifying the affected individuals at risk of serious harm, the Office of the Australian Information Commissioner (OAIC) and the Department of Jobs and Small Business (the Department).

It is important to note that not all incidents involving unauthorised access to or disclosure of personal information would be considered an 'eligible data breach' and so an assessment must be made for each case to determine whether the requirements of the NDB scheme apply.

Who is responsible for managing a breach?

Employment services providers are responsible for managing incidents of privacy breaches involving personal information held by their organisation or by a third party with which they have shared this information.

This includes, in accordance with the NDB scheme, assessing whether serious harm has occurred or is likely to occur, and whether notification to affected individuals and to the OAIC is required

Provider are also responsible for ensuring arrangements are in place within their organisations to comply with the NDB scheme. This includes preparing or updating their data breach response plan to ensure they are able to respond quickly to suspected data breaches, and conduct an assessment as required under the NDB scheme.

When is a privacy incident considered an 'eligible data breach'?

An 'eligible data breach' has occurred when:

1. there is unauthorised access, disclosure, or a loss of personal information
2. this is likely to result in serious harm to one or more individuals, and
3. the likely risk of serious harm could not be prevented with immediate remedial action.

If these criteria are met, the provider must undertake mandatory notification to affected individuals and to OAIC.

Guidance for determining whether a privacy incident is an 'eligible data breach' is available from the OAIC website.

How to decide if the breach will cause serious harm?

Providers need to decide from the perspective of a reasonable person, whether a breach would likely result in serious harm to the affected individuals. The phrase 'likely to result' means the risk of serious harm to an individual is more probable than not (rather than possible). The assessment should be based on, but is not limited to, the following factors:

a. the kind of information involved
b. the sensitivity of the information
c. the availability of security measures protecting the information and the likelihood that the security measures could be overcome
d. the type of people who could obtain the information and whether they may have the intention of causing harm to any of the affected individuals
e. the nature of harm that could be inflicted on the affected individuals.

Further information is available on the OAIC website.

Who should be notified when a privacy breach occurs?

All incidents involving the loss, unauthorised access to, or unauthorised disclosure of, personal information involving the Department's employment services programs must be reported to your Account Manager at the Department.

This reporting requirement applies whether or not the incident qualifies as an 'eligible data breach'.

Where a provider suspects that an 'eligible data breach' has occurred, further notification must be given to any affected individuals and OAIC.

Notification must be made as soon as practicable and may be given by the usual means of communication with jobseekers, such as email.

What actions are required when a privacy breach occurs?

There are three immediate actions providers should take when an incident involving the loss, unauthorised access to, or unauthorised disclosure of, personal information has occurred, or could occur:

1. **Contain the breach** – determine and take appropriate steps to contain a breach of person information, including steps to limit any further access or distribution of affected personal information, or the compromise of other information.
2. **Conduct an initial assessment** – determine if a breach may result in likely serious harm to any affected individual, considering any immediate action taken to contain or remedy the breach. If so, prompt notification to OAIC and the individual(s) must be undertaken, including when this may reduce any harm or risk of harm, or assist to contain the breach.
3. **Notify the Department** – provide immediate notification to your Account Manager about a breach and the actions undertaken to contain or remedy the breach.

A full assessment of the incident must then be undertaken within 30 calendar days to determine whether the incident is an 'eligible data breach' under the NDB scheme.

This assessment also requires consideration of further actions required to contain the breach and what notifications (or additional notifications) are required to affected individuals and OAIC.

Guidance for conducting an assessment of an incident under the NDB scheme is available from the OAIC website.

Note: The commencement of the NDB scheme in no way varies the existing obligation of providers to immediately notify the Department and manage any actual or suspected breach of privacy involving personal information which does not qualify as an eligible data breach under the NDB scheme.

Are resources available?

The OAIC website provides extensive guidance on the NDB scheme, including the steps you are required to undertake when personal information has been lost, or an incident of unauthorised access or disclosure of personal information has been identified. The guidance includes requirements for the assessment of a breach incident and the notification obligations when an 'eligible data breach' is found.

All provider staff who may identify or manage a data breach incident should be encouraged to review the resources available from the OAIC website to ensure they are familiar with the requirements of the NDB scheme and can effectively discharge their responsibilities under the scheme.

The Department has also updated the following resources to reflect the requirements of the NDB scheme:

- The Learning Centre module on Exchange of Information and Privacy
- The Employment Service Provider Privacy Guideline.

Further information

The Office of the Australian Information Commissioner administers the NDB scheme and offers extensive guidance and resources on its website (www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme).