POLICY No 35. – Privacy and Confidentiality

Background:

Pines Learning respects and values the privacy of all individual's personal information and we are committed to handling all personal information consistent with our obligations under the Australian Privacy Principles (March 2014) and the Information Privacy Act 2000. Pines Learning is obligated to comply with the notifiable data breaches scheme under the Privacy Amendment Act 2017 (NDB scheme) as it is contracted by the Commonwealth government to provide childcare services.

Purpose:

1. To set out how and what information is collected, maintained, disclosed and disposed.
2. To ensure compliance with the Information Privacy Act 2000 and Health Records Act 2001.
3. To ensure personal information is used for the purpose for which it is collected and safeguarded from misuse.
4. To outline what constitutes an eligible data breach and how it is determined.
5. How, when and to whom to notify in the event of an eligible data breach.

Distributed to: Board members, Staff, Trainers, Volunteers, Learners, Childcare Users

Applicability: This policy encompasses all methods of collecting personal information including hard copy, electronic or verbal. It applies to all Board members, employees paid and unpaid who access any personal information of past, present, potential Centre users, employees or Board members.

Related Documents:

G:\LEGISLATION\APP_guidelines_complete_version_1_March_2014.pdf
www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles
www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Pines Learning Cybersecurity Strategy (G:\RISK MANAGEMENT\Pines Learning Cyber Security Strategy.docx)

Pines Learning Archiving procedure (G:\RECORDS MANAGEMENT\Archiving Procedures (2).docx)

Definition:

Confidential – Information that is secret, private, or shown in trust. Information between two people is confidential if it is given with the expectation that it will go no further.

Privacy - the state of being free from public scrutiny or from having your secrets or personal information shared. The kind of information rather than the relationship between the person giving it and the one receiving it. Information is private if it is sensitive or personal in some way. Here, privacy is taken as referring to a person's interest in limiting the disclosure and dissemination of private information.

Data breach – a security incident in which sensitive, protected or confidential information is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so

Eligible data breach – where unauthorised access, unauthorised disclosure, or loss of personal information is likely to result in serious harm to one or more individuals affected.

Unauthorised access of personal information occurs when a person accesses this information who is not authorised to do so. This can include unauthorised access by an employee, an independent contractor or an external hacker.

Unauthorised disclosure of personal information occurs when an organisation makes personal information accessible or visible to others outside the organisation.

Loss refers to the accidental or inadvertent loss of personal information held by an organisation in circumstances where it is likely to result in unauthorised access or disclosure.

Likely to involve serious harm refers to the risk of serious harm to an individual is more probable than not as assessed by the Centre Manager in consultation with the Board members who have been informed based on the information immediately available or information that could be obtained following reasonable enquiries.

The NDB scheme provides the following examples to be taken into account when deciding whether a data breach is likely to result in serious harm:

Factors	**Examples of less serious breach**	**Examples of more serious breach**
The kinds of information involved and the sensitivity of the information	Name (without other linking information)	HIV status Driver licence Credit card information Multiple types of personal information
Whether the information is protected by one or more security measures and the likelihood those measures could be overcome.	Reputable encryption by software	No encryption Standard Windows password
The persons, or the kinds of persons, who have obtained, or who could obtain, the information.	Internal employee trained in safe treatment of personal information receives a confidential client file in error.	Disclosure to public Access by hackers
The nature of the harm	Information previously available publicly	Identity theft Financial loss Physical safety Reputational damage Humiliation
Remedial action	Organisations may not need to notify if they take positive steps to address a data breach in a timely manner. To avoid the need to notify, the remedial actions need to be effective enough so that the organisation believes that the data breach will no longer likely result in serious harm.	If the remedial action only prevents the likelihood of serious harm to some individuals within a larger group of individuals whose personal information has been compromised, the organisation still needs to notify the affected individuals who will likely experience serious harm.

Policy:		**Responsible party**
1.	**What information is collected and why**	**All staff**
i	Pines Learning collects personal information in relation to its paid and unpaid employees, board members, learners and childcare users.	
ii	Pines Learning only collects personal and health information that is required to provide learners and childcare users with services that meet their needs.	
iii	Pines Learning's contractual obligations to various regulatory and funding government departments require the collection of information in	

	relation to Board members, paid and unpaid employees, learners and childcare users. This information includes, but is not limited to: Name, home address, contact details, gender, date of birth, nationality, personal background, employment category health issues, educational qualifications and emergency contacts.	
iv	Pines Learning requires contact details to enable communications between relevant parties. For example, if courses are cancelled or postponed and general occupational health and safety.	
v	Pines Learning requires personal and health information from employees both paid and unpaid to meet requirements of the workplace, such as: communication, WorkCover, and occupational health and safety.	
vi	Any information marked as confidential will only be accessed by authorised people and disposed securely when no longer required.	
2.	**How personal information is collected**	**All staff**
i	Directly from the person providing the information through employment forms, enrolment forms, online applications or enquiries.	
ii	Other persons, agencies, schools or education providers with authority to provide personal information on another person's behalf.	
iii	Information provided by a third party, Pines Learning will seek clarification from the individual to ensure accuracy.	
iv	Pines Learning will endeavor to ensure information is accurate prior to using it.	
v	We rely on each person to provide accurate information. When details change we expect people to advise us asap.	
3	**How personal information is maintained and stored**	**All staff**
i	Current completed enrolment forms are stored in a secure office area accessible only by authorised staff.	
ii	For current learners undertaking accredited courses, learner files are coded and stored in a secure office area accessible only by authorised staff.	
iii	For current paid and unpaid employees, employment files are coded and stored in a secure office area accessible only by authorised staff.	
iv	Learner and employee files no longer current are stored securely in a compactus and subsequently archived according to the archiving procedure (G:\RECORDS MANAGEMENT\Archiving Procedures (2).docx)	
v	Pines Learning implements the following safeguards to ensure online information is secure: • VETtrak is the database used to store personal information and is password protected • Up to date virus protection and a firewall on the server that houses all data • Spam filters to ensure no unauthorised breaches of data access • Encrypted Back up of data daily	
4	**How is personal information disclosed**	**All staff**
i	Pines Learning will not disclose information unless required to do so by a legal authority.	
ii	The legal authorities may include:	

	• government departments or agencies as part of our legal and funding obligations • local government authorities, for planning purposes • organisations providing services related to employee entitlements and employment • insurance providers, in relation to specific claims or for obtaining cover • law enforcement agencies • health organisations and /or families in circumstances where the person requires urgent medical assistance and is incapable of giving permission • anyone to whom the individual authorises us to disclose information.	
iii	When personal details/information about a learner is requested by another party or organisation, written consent must be obtained from the learner. A separate procedure is followed to gain consent prior to disclosing personal information. G:\PROCEDURES\Disclosure of Learner Information.doc	
iv	Information is not disclosed to any person or organisation located in a foreign country unless prior consent is provided by the individual. The procedure indicated in point 4iii must be followed.	
v	Individuals can access their own information by completing the following form: G:\PROCEDURES\VET specific procedures\learner request for records formv4.docx available by contacting reception or downloaded from our website.	
5	**Complaints**	**CM**
i	There are a range of options available to lodge a complaint in regard to privacy and confidentiality breaches: • By phone - Centre Manager on 9842 6726 • In writing to: Centre Manager – Pines Learning 1/520 Blackburn Road Doncaster East 3109 • Email - Centre Manager on info@pineslearning.com.au • Using a downloadable form as per our complaints policies: G:\POLICIES\Organisational Policies\CURRENT\Complaint Form v3 as per Policy 28, 29.docx Complaints policies are available through the appropriate handbooks or induction kits. Complaints individuals feel were not appropriately dealt with by Pines Learning can be referred to: The Privacy Commissioner Privacy Victoria GPO Box 5057	

	Melbourne, 3001 Or email: enquiries@privacy.vic.gov.au	
6	**How personal information is disposed**	**All staff**
i	Each program area of the organisation is bound by different record archiving guidelines. A complete records management procedure exists to detail these. G:\RECORDS MANAGEMENT\Archiving Procedures (2).docx	
ii	All files containing personal information are destroyed securely.	
7	**Suspected Data Breaches**	
i	If Pines Learning suspects that it has experienced an eligible data breach it will undertake a prompt investigation to assess whether or not the breach is reportable.	
ii	Pines Learning will not delay its investigation in point 7i and will notify Board members via email asap. The assessment will not exceed 30 days from the date of suspicion.	

iii	The assessment of a suspected data breach will be undertaken in 3 stages:
	• **Initiate**: identify the person or group responsible for completing the assessment
	• **Investigate**: gather all the relevant information about the data breach, eg
	  ○ Can we employ any remedial action?
	  ○ What personal information has been affected?
	  ○ Who may have had access to it?
	  ○ What are the likely impacts?
	• **Evaluate**: the person or group needs to make a decision as to whether it is a notifiable data breach. This decision should be well documented, including the reasons why that decision was reached.	

iv	If Pines Learning believes it has experienced an eligible data breach it will proceed to notification section 8.	
8	**Notification of Data Breaches**	**CM**

i	If Pines Learning believes an **eligible data breach** has occurred, the organisation must:
	• Contain the breach in so far as is possible
	• Prepare a notification statement that contains:
	  ○ the identity and contact details of Pines Learning
	  ○ a description of the data breach (date, cause, who most likely has the data, steps taken to contain and remedy breach)
	  ○ the kinds of information affected (eg name, contact details, credit card, health, passport numbers etc)
	  ○ recommendations for affected individuals (eg cancel credit cards advise passport office etc)
	• Provide a copy of the notification statement to the OAIC (Office of the Australian Information Commissioner) details in section 8v.
	• Quickly notify individuals at likely risk of serious harm.	

ii	If Pines Learning considers that a data breach will result in serious harm to one or more individuals but cannot assess which individuals are at risk, it will notify all affected individuals.	
iii	Individuals detailed in point 8ii will be notified asap and within 30 days to mitigate the effect of the breach.	
iv	If the individuals to be notified in point 8iii are under 18 years of age their parent or guardian will also be notified.	
v	Notifications detailed in points 8iii – 8iv will be undertaken by the Centre Manager and will take the form of: • Phone or • Email or • Letter	
vi	Eligible data breaches will be reported to the Office of the Australian Information Commissioner within 30 days. Contact details for the OAIC are: 1300 363 992 enquiries@oaic.gov.au www.oaic.gov.au GPO Box 5218, Sydney NSW 2001	