



DATA BREACH POLICY

Document No:	HR Policy 25
Publication Date:	November 2018
Replaces Document:	Nil
Contact:	Human Resources Phone: 8508 3308 Email: hr@johnpaulvillage.com.au
Review Date:	2 years (or earlier, where required).
Status:	Active

DATA BREACH POLICY

1. INTRODUCTION AND PURPOSE

John Paul Village (JPV) is responsible for demonstrating accountability and responding promptly in the event a Data Breach occurs.

The purpose of this policy is to outline the JPV Data Breach Response Plan to provide guidance to Employees, Contractors and Managers, and specifies the step by step actions required.

2. SCOPE

This policy applies to all employees, contractors and volunteers engaged by JPV.

3. DEFINITIONS

Data breach is unauthorised access, disclosure or loss of personal information. It can be malicious (external or internal), human error or a failure in information handling or security systems. A data breach can cause serious harm to the individual whose personal information is lost. Examples of serious harm include: physical, mental, well-being, financial loss or damage to reputation. A data breach can be to one individual or company or can be to multiple individuals or companies. An assessment of a data breach will be completed to determine the severity of a data breach. A data breach can also negatively impact the reputation of a company and its ability to protect private information.

Data Breach Manager is the ILU Manager or another delegated person.

4. PROCEDURE & RESPONSIBILITIES

4.1 DATA BREACH RESPONSE PLAN

The Data Breach Response Plan provides clarity regarding the roles and responsibilities of Managers and Employees. The response to a data breach should be quick and measured to reduce the impact on the affected individuals, reduce cost associated with dealing with the data breach and ensures JPV meets their obligations as outlined in the *Privacy Act 1988 (Cth)*, *Privacy Amendment (Notifiable Data Breaches) Act 2017* and the *General Data Protection Regulation*.

JPV is responsible for the education and regular testing of the Data Breach Response Plan to ensure employees are aware of how to respond in the event of a data breach.

Assessment of a Data Breach

In the event of a data breach the employee who identified the data breach is responsible for notifying their manager and completing an assessment of the data breach. The employee is responsible for providing an accurate and timely report of the incident. The employee will have 24 hours to report an incident to management.

The employee should assess the below and report to their manager (utilising the Data Breach Incident Report):

- How did the breach occur?
- Is the information still being shared, disclosed or lost without authorisation?
- Who has access to the potential information?
- What can be done to secure this information, stop unauthorised access or disclosure and reduce the risk of harm to individuals?
- Management are required to set a meeting with the identifying employee to discuss the incident. The Manager will record further details surrounding the data breach and determine the below:
 - How many people have been affected by the breach or suspected breach?
 - Is there a risk of serious harm to affected individuals now or in the future?
 - Does the data breach or suspected data breach indicate a systemic problem with the company practices or procedures?
 - Does the risk impose a significant value of the data to you or issues of reputational risk?
- Management is required to escalate and provide the completed Data Breach Incident Report to the Data Breach Manager.

The Responsibility of the Data Breach Manager

The Data Breach Manager is responsible for carrying out actions to reduce the potential risk. The Data Breach Manager will ensure accurate and timely recording of each data breach incident and assessing the level of risk.

A guide on assessing the risk level is outlined below:

Likelihood of occurrence	Severity of Impact/Consequences		
	Minor	Moderate	Major
Frequent	Medium	High	High
Occasional	Low	Medium	High
Improbable	Low	Low	Medium

The Data Breach Manager may need to obtain external advice depending on the severity of the breach including Legal, Media & Public Relations.

Reporting a Data Breach Incident

Staff should be mindful at all times of the privacy of residents and/or clients data at all times. If a staff member becomes aware of a potential breach, then they are responsible for notifying their manager and completing an assessment of the data breach within 24 hours.

The Data Breach Manager or delegated person is responsible for:

- ensuring the Data Breach Incident Report is completed by the Employee and the Manager;
- notifying the insurance company and complete any necessary steps the insurance policy may require;
- notifying law enforcement, regulators, or any required entity of data breaches; and
- recording a current list of members of the response team.
- The Data Breach Incident Report should be accessible to Management and Employees on the Q drive

Eligible Data Breach

A data breach is classified as eligible if it meets the following criteria:

- Unauthorised access or unauthorised disclosure of personal information, or a loss of personal information;
- It is likely to result in serious harm to one or more individuals;
- Remedial action taken by the company has not prevented the risk of harm.

Exceptions may apply when determining an eligible data breach and should be assessed on a case by case basis.

What is Remedial Action?

Remedial action is the steps taken following the identification of a data breach to remove the risk caused by the breach. If the remedial action is successful in removing the likelihood of the data breach resulting in serious harm. The data breach is then no longer deemed as eligible and is longer required to be responded to. Remedial action is adequate if it prevents unauthorised access to, or disclosure of personal information.

Examples of Remedial Action

Data Breach Incident	Remedial Action Taken
Email containing sensitive information sent to the incorrect person.	Sender contacts the individual whom has received the email asks them to confirm they have permanently deleted the file and not copied the information.
Lost smartphone/laptop.	IT have remotely removed sensitive access including email and programs from the device successfully.

Responding to Data Breaches

Each data breach will be assessed and dealt with on a case-by-case basis. Depending on the severity of the breach, the risks associated, and the number of people affected. All data breaches are required to be contained, assessed and the required individuals notified. A review of the incident should be conducted to ascertain what actions can be taken to prevent further breaches.

A communication strategy may need to be put in place to ensure all breaches are communicated effectively.

Guidelines on how to communicate and notify the affected individual/s and/or company are outlined below:

- Obtain contact details;
- Provide a description of the data breach and the grounds of how it is believed to have happened;
- Inform the nature of the information concerned
- Advise recommendations the affected individuals should take;
- A notification must be provided in a timely manner.

Depending on the severity JPV may be required to:

- notify affected individuals who has had their personal data involved in the data breach;
- notify individuals who are at risk or at harm;

- Publish your notification, and publicise it with the aim of bringing it to the attention of all individuals at key risk e.g. relevant company website, social media page and public service announcement on either television, radio, newspaper;
- Notify law enforcement should criminal activity be involved in the breach;
- Notify Human Resources where an individual is responsible for a large data breach and disciplinary action is required.

A notification may also be required to be sent to the Australian Information Commissioner of the data breach under the NBD scheme. If a Data Breach is deemed eligible a company must notify the Commissioner via a statement. This can be done through OAIC's Notifiable Data Breach form which can be found at <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme> This link also provides supporting data regarding the Notifiable Data Breaches Scheme

The Commissioner requires all steps to assess, respond and notify should be completed within 30 days of the incident being reported.

Date Breach Response Summary

Review of Data Breach

A review of the data breach must be completed within 30 days of the initial breach notification. The review should be completed by the Data Breach Manager or delegated person, and should include the below:

- How did the breach occur?
- Success of response?
- Can we improve our data handling?
- Can we improve data breach management?

4.2 EU – GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR applies to all companies possessing the personal data of European Union (EU) nationals and relates directly to the personal data of EU nationals a company has access to.

In the case of an EU Personal Data Breach, the Data Breach Manager must advise the Australian Information Commissioner of the data breach, 72 hours after becoming aware of it. That is, unless the personal data breach is deemed unlikely to result in a risk to the person. If the notification to the OAIC is not within 72 hours, the Data Breach Manager must outline the details of the delay.

GDPR, breaches can only involve a breach of security to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

All EU Personal Data Breaches, regardless of the severity must be recorded and if the breach will cause risk to the person and notification is required upon the severity of the breach. An investigation to see if the personal data was a breach must be completed by the Data Breach Manager and notification must be completed if a risk to an individual is deemed.

Use of the OAIC's Notifiable Data Breach form needs to be completed and submitted.

5. BREACH OF POLICY

A breach of this policy will be dealt with seriously and may result in disciplinary action, up to and including termination. For contractors who are found to have breached this policy, there may be consequences including termination of contract. Where inappropriate use under this policy constitutes a breach of any law, action may also be taken in accordance with that law by JPV.

6. ASSOCIATED LEGISLATION

- Privacy Act 1988 (Cth),
- Privacy Amendment (Notifiable Data Breaches) Act 2017; and
- General Data Protection Regulation.

7. ASSOCIATED DOCUMENTS

- Privacy Policy
- IT Policy
- Data Breach Incident Report Form

8. FURTHER INFORMATION

Further information about this document can be sought from Human Resources by telephone on 8508 3308 or email on hr@johnpaulvillage.com.au John Paul Village reserves the right to change this policy from time to time.