**[Charity name]**

**Plan for responding to a data breach**

Responding to a data breach

A data breach is when protected information is accessed or disclosed without authorisation. People in your charity should know what to do when a data breach occurs. This plan template will help you to outline the steps for responding to a data breach, and assign roles for dealing with each step. The people responsible for each action of the plan will be in charge of making sure the plan is followed.

This plan template is a starting point and can be changed to suit your charity’s needs.

Once you complete your charity’s plan, make it available to the people responsible for each action so they can be prepared to respond to a data breach.

| **Step** | **Action** | **Person responsible** |
| --- | --- | --- |
| 1. Identify
 | Report the actual or suspected data breach immediately to **[name]**. |  |
| Decide whether an actual or suspected data breach has occurred. [Use the [OAIC guide](https://www.oaic.gov.au/privacy/notifiable-data-breaches/) to identify if an eligible data breach has occurred or not]. |  |
| Appoint someone as the response co-ordinator if an actual data breach has occurred. |  |
| The individual who discovered the breach should take note of the following details, and pass the information to the co-ordinator:* The time and date of the actual or suspected data breach
* The type of information involved
* Ways the data breach can be contained
 |  |
| 1. Investigate
 | Investigate the breach and assess:* The information involved in the data breach
* The cause of the breach
* The extent of the breach
* People who have been, or may be, affected
* The extent of the harm
* The need to notify the people affected, and what information they need to know.
 |  |
| 1. Assess
 | Assess each threat identified from the breach based on the information gathered during the investigation. This assessment should consider whether:* There has been any loss, misuse or disclosure of information
* There is a risk of harm to individuals because of the breach (for example, has it revealed personal or sensitive information?)
* Actions have been taken to reduce the risk of harm
* There is a need to notify affected people or relevant regulators
 |  |
| Record the details of the assessment and keep it filed (physically or electronically). Make sure people who need to see it get a copy or can access it easily. |  |
| 1. Notify
 | Notify the affected people, organisations and regulators. Consider whether:* The notification needs to happen within a set timeframe
* The notification needs to be in a particular format (for example, an email or a letter)
* Your charity wants to publish a public notification on its website or social media pages
 |  |
| 1. Review
 | Review the data breach and the response. Record the findings and make a list of recommendations for improvements. Make sure the review covers the following:* An understanding of how the breach occurred
* Updates to processes for managing information and data to prevent another breach occurring
* Updates to systems or technology if the breach was due to a technical vulnerability
* Updates to other relevant policies and procedures to reflect changes
* Employee training for dealing with the private and confidential information
 |  |