Cloud Paper Group Pty Ltd
Data Breach Response Plan

Introduction

The passage of the Privacy Amendment (Notifiable Data Breaches) Act 2017 established the Notifiable Data Breaches (NDB) scheme in Australia. The NDB scheme applies to all agencies and organisations with existing personal information security obligations under the Australian Privacy Act 1988 (Privacy Act) from 22 February 2018.

The NDB scheme introduced an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches.

This Data Breach Response plan (response plan) sets out procedures and clear lines of authority for Cloud Paper Group (CPG) staff in the event that CPG experiences a data breach (or suspects that a data breach has occurred).

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

This response plan is intended to enable CPG to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals. It sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist the CPG to respond to a data breach.

CPG manages personal information on behalf of its customers. It is important to stress that the data does not belong to CPG, it belongs to the customer, and consequently any breach of customer data must be communicated to the customer.

Our standard practice is CPG will never communicate directly with people who are contained in customer data - for example parents, students and staff of a school - without the explicit permission of the customer. The exception is where in our view a notifiable breach has occurred and the school does not have the mechanisms to readily target notifications to the affected people, and CPG must discharge its obligation under the Act to notify individuals at likely risk of harm.

CPG will ask all customers to provide a contact person who will be the customer's liaison with CPG in the event of a data breach.

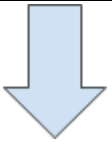
This plan was modelled on the one provided by the Office of the Australian Information Commissioner, available on their web site.

Plan Stages

Stage 1: Data breach suspected or notified

Responsibility: All Staff
Time frame: Immediately

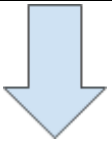
Either a staff member or customer discovers that a breach may have occurred. Immediately notify CEO and CTO, document via phone, email with attachment.



Stage 2: Evaluation of the breach

Responsibility: Chief Technology Officer
Time frame: Within 30 days

Evaluate if a breach has occurred, or is likely to have occured. Determine what response is required. If a notifiable breach is believed, or suspected, escalate to Stage 3.



Stage 3: Implement Data Breach Response

Responsibility: Response Team - Chair, CEO and CTO
Time frame: Within 7 days

Implement Notifiable Data Breach Response plan

Key Contacts

Current at January 2018.

Chair	CEO	CTO
Tim Fry tim@edsmart.com	Fiona Boyd fiona@edsmart.com	David Eedle david@edsmart.com

Stage 1: Data breach suspected or notified

If a staff member discovers that a breach may have occurred (or is notified by a customer), they must immediately notify CEO and CTO, in person/by telephone and document via email and attachment as much detail as is known including:

- Name of School/Customer
- Name(s) of affected people, if known
- Evidence of breach - copies of any material which might constitute a breach

Evaluation of the breach

The CTO will take responsibility for evaluation of the breach:

- Evaluate if a breach has occurred, or is likely to have occured
- Document evaluation outcomes
- Determine if a breach has occured

What constitutes a data breach?

- An eligible data breach occurs when three criteria are met:
    - There is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds
    - This is likely to result in serious harm to one or more individuals, and
    - The entity has not been able to prevent the likely risk of serious harm with remedial action
- ‘Serious harm’ can be psychological, emotional, physical, reputational, or other forms of harm
- Understanding whether serious harm is likely or not requires an evaluation of the context of the data breach.

When should the CTO escalate a data breach?

The CTO may use discretion in deciding whether to escalating the breach to Step 3. Some data breaches may be comparatively minor, and able to be dealt with easily without escalation.

For example, it might be discovered either a member of CPG staff, or a customer, may as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the sender can contact the recipient and the recipient agrees to delete the email, it may be that there is no utility in escalating the issue.

The CTO should use their discretion in determining whether a data breach or suspected data breach requires escalation. In making that determination, the CTO should consider the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in CPG processes or product?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is ‘yes’, then it may be appropriate for the CTO to escalate the issue to Step 3

CTO to document minor breaches

If the CTO decides not to escalate a minor data breach or suspected data breach the CTO should create an incident report document, saved on the CPG Google Drive, containing:

- description of the breach or suspected breach
- action taken by the CTO to address the breach or suspected breach
- the outcome of that action, and
- the CTO’s view that no further action is required

Stage 3: Implement Data Breach Response

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

There are four key steps to consider when responding to a breach or suspected breach.

STEP 1: Contain the breach and do a preliminary assessment
STEP 2: Evaluate the risks associated with the breach
STEP 3: Notification
STEP 4: Prevent future breaches

The response team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession.

Step 1: Contain the breach and make a preliminary assessment

- Convene a meeting of the data breach response team
- Immediately contain breach - for example, if emails are still in queue, stop the queue and delete
- Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing CPG to take appropriate corrective action
- If the breach involves customer data immediately establish contact with customer staff member designated as the data breach contact; in absence of a specific contact, the primary Administration contact for the customer

Step 2: Evaluate the risks for individuals associated with the breach

- Conduct initial investigation, and collect information about the breach promptly, including:
    - the date, time, duration, and location of the breach
    - the type of personal information involved in the breach
    - how the breach was discovered and by whom
    - the cause and extent of the breach
    - a list of the affected individuals, or possible affected individuals
    - the risk of serious harm to the affected individuals
    - the risk of other harms
- Determine whether the context of the information is important
- Establish the cause and extent of the breach
- Assess priorities and risks based on what is known
- Keep appropriate records of the suspected breach and actions of the response team, including the steps taken to rectify the situation and the decisions made
- Provide this information to the customer

Step 3: Consider breach notification

- Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage
- Discuss with customer and determine whether to notify affected individuals – is there a real risk of serious harm to the affected individuals? In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals
- Consider whether others should be notified, including police/law enforcement, or other agencies or organisations affected by the breach, or where CPG is contractually required or required under the terms of a contract or similar obligation to notify specific parties
- Determine whether notification to the Australian Information Commissioner is required. If it is required, provide a copy of the notification to the customer.

School Contacts

CPG will request that all of its customers advise the appropriate contact person with whom CPG will liaise in the event of a data breach. Where a school has not provided this contact person, CPG will liaise with the Account Administrator as designated in CPG Admin System.

Who to Notify

Under the Act CPG must notify any individuals that are at likely risk of serious harm as a result of a data breach. CPG must also notify the Australian Information Commissioner.

There are three options for notification:

- Notify all individuals whose personal information is involved in the eligible data breach
- Notify only the individuals who are at likely risk of serious harm; or
- Publish your notification, and publicise it with the aim of bringing it to the attention of all individuals at likely risk of serious harm

CPG will make a decision about which is the most appropriate option on consultation with the affected school.

Notification to the Australian Information Commissioner

There is an online form to notify the Commissioner:

https://forms.uat.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

Step 4: Review the incident and take action to prevent future breaches

- Fully investigate the cause of the breach
- Report to CPG Board on outcomes and recommendations:
    - Update security and response plan if necessary
    - Make appropriate changes to policies and procedures if necessary
    - Revise staff training practices if necessary
    - Consider the option of an audit to ensure necessary outcomes are effected
- Report to the customer in summary of the outcomes and recommendation

Further Information

- Notifiable Data Breaches scheme at Office of the Australian Information Commissioner
- Information Commissioner Webinar Slides