



# Cyber Security & Response Plan Policy and Procedure



Policy number	12	Version	1
Drafted by	Janiece Stark	Approved by Board on	2024-08-22
Responsible person	File Management Officer	Scheduled review date	2026-08-22

## Background/Introduction

Days for Girls Australia Limited (DfGAL) is committed to providing a safe environment when working with online, connected to an intranet or internet.

## Purpose

This Response Plan sets out procedures and clear lines of authority for Board members who experience a data breach (Or suspects a data breach has occurred)

“[oaic](#) definition:- “A data breach happens when personal information is accessed, disclosed without authorization or is lost. For example when:

- A USB or mobile phone that holds a individual’s personal information is stolen
- A database containing personal information is hacked
- Someone’s personal information is sent to the wrong person
- A data breach can harm an individual whose personal information is affected. They can, for example, suffer distress or financial loss.”

Data breaches result in CONFIDENTIAL DATA held by the Association ending up in the hands/systems of unauthorised third parties and give rise to a range of actual or potential harms to individuals, agencies and organisations. A data breach can be accidental, unintended or malicious action.”

## Policy

This response plan is intended to enable us 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

people in the event of a data breach, clarifies the roles and responsibilities, and documents processes to enable a rapid and appropriate response to a data breach.

A Response team should be led by the Chair and the Chief Operations Officer (COO), adding in those Board members or other team members based on need. The COO should inform Days for Girls International (DfGI) and involve the Information Technology (IT) team.

## Procedure

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 for the Breach Response Team 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 simultaneously or in quick succession.

The following checklist is intended to guide the response team in the event of a data breach and alert the response team to a range of considerations when responding to a data breach.

### STEP 1:

- Contain the breach and do a preliminary assessment
- DfGI IT conduct initial investigation and discovery — if necessary contain the breach (i.e. disabling internet, shutting down server/s, locking user account/s) — and answer these initial points:
  - What personal information does the breach involve?
  - What was the cause of the breach?
  - What is the extent of the breach?
  - What are the harms that could potentially be caused by the breach?
- How can the breach be contained?
- Ensure evidence is preserved that may be valuable in determining the cause of the breach or allowing the Association to take appropriate corrective action.
- Convene a meeting of the data breach response team.
- Consider developing a communications or media strategy to manage public expectations and media interest.

### STEP 2:

- Evaluate the risks associated with the breach
- Conduct/continue initial investigation, and collect information about the breach promptly above what has already been discovered or adding detail to information already discovered, 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

- o the cause and extent of the breach
- o a list of the affected individuals, or possible affected individuals
- o the risk of serious harm to the affected individuals.
- Determine whether the context of the information is important.
- Determine how the information could be used to cause harm — examples of serious harm:
  - o identity theft
  - o financial loss • threat to physical safety
  - o threat to emotional wellbeing
  - o loss of business or employment opportunities • humiliation, damage to reputation or relationships, or
  - o workplace or social bullying or marginalisation.
- Establish the cause and extent of the breach.

### STEP 3:

- Determine who needs to be made aware of the breach (internally and potentially externally).
- Determine whether to notify affected individuals — is there a real risk of serious harm to the affected individuals? If serious enough, it may be appropriate to notify the affected individuals immediately.
- NOTIFY affected clients via call/letter/email/person based on above findings.
- NOTIFY the OAIC (Office of the Australian Information Commissioner) of the breach via:
  - o 1300 363 992
  - o enquiries@oaic.gov.au
- Notification to clients/OAIC should be very similar — the detail/information to include is detailed below

### STEP 4.

- Consider whether others should be notified, including police/law enforcement, our insurance providers or other agencies or organisations affected by the breach (or that could possibly be affected by the breach/vector).
- Prevent future breaches
- Fully investigate the cause of the breach.
- Report to the Board/COO on outcomes and recommendations:
- Update security and response plan if necessary.
- Make appropriate changes to policies and procedures if necessary.
- Revise Board Directors/volunteers induction and training practices if necessary.
- Keep Board/COO aware of progress/implementation of any changes/solutions.

### What should be included in the Notification?

The content of notifications will vary depending on the particular breach and the notification method. In general, the information in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Notifications should include the types of information detailed below:

- Incident Description — Information about the incident and its timing in general terms. The notice should not include information that would reveal specific system vulnerabilities.
- Type of personal information involved — A description of the type of personal information involved in the breach. Do not include any personal information in the notification.
- Response to the breach — A general account of what has been done to control or reduce the harm and proposed future steps that are planned.
- Assistance offered to affected individuals — What will be done to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves. For example,

whether the agency or organisation can arrange for credit monitoring or other fraud prevention tools, or provide information on how to change government issued identification numbers.

- Other information sources — Sources of information designed to assist individuals in protecting against identity theft or interferences with privacy. For example, guidance on the OAIC’s website and the Attorney-General’s Department website at Identity security.
- DfGAL contact details — Contact person for DfGAL that can answer questions, provide further information or address specific privacy concerns.
- DfGAI contact details - Contact person for DfGAL that can answer questions, provide further information in relation to internet/email or address specific privacy concerns.
- Whether breach was notified to regulator or other external contact(s) — Indicate whether DfGAL notified the OAIC, police or other external parties about the breach/incident.
- How individuals can lodge a complaint with DfGAL— Provide information on internal dispute resolution processes and how the individual can make a complaint to DfGAL or industry complaint handling bodies.

Authorised DfGAL Board on - 2024-08-22  
Uploaded to Shared Drive in PDF - 2024-09-04

## Cyber Security Breach Form

DATE OF ENTRY:	TIME OF ENTRY:	Responsible Person:
DATE AND TIME INCIDENT DETECTED		
CURRENT STATUS	New / In Progress / Resolved	
INCIDENT TYPE		
INCIDENT CLASSIFICATION	Incident / Significant Incident / Emergency	
SCOPE - list the affected affected networks, systems and/or applications; highlight any change to scope since the previous log entry		
IMPACT - list the affected stakeholder(s); highlight any change in impact since the previous log entry		
SEVERITY - outline the impact of the incident on the stakeholder(s); highlight any change to severity since the previous log entry		

NOTIFICATIONS ACTIONED/PENDING	
ADDITIONAL NOTES	
CONTACT DETAILS FOR INCIDENT MANAGER	
DATE AND TIME OF NEXT UPDATE	



DAYS FOR GIRLS AUSTRALIA LIMITED  
 DAYSFORGIRLS.ORG/AUSTRALIA  
 ABN 77 599 800 484  
 @DAYSFORGIRLSAUSTRALIA  
 PO BOX 179, TATURA VIC 3616  
 australia@daysforgirls.org

## Cyber Security Breach Resolution Action Plan Form

DATE AND TIME	CATEGORY (Contain / Eradicate / Recover / Communications)	ACTION	ACTION OWNER	STATUS (Unallocated / In Progress / Closed)

