

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



## 1. Purpose

- 1.1 When stakeholders disclose their personal information to us, they are placing trust in Deutsche Schule Melbourne (**the School**) to protect their personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
- 1.2 The School is required to keep personal information safe and secure in accordance with strict legal obligations and it is our expectation that all staff members assist the School to comply with its obligations.
- 1.3 This Data Breach Response Plan (**Plan**) applies to all employees, contractors and volunteers engaged by the School and is to be applied in the event that a data breach occurs, or is suspected to have occurred.
- 1.4 It is essential that all employees, contractors and volunteers are proactive in responding to a data breach incident and that they take such preventative action necessary before any serious harm occurs to the affected individuals.

## 2. What sort of personal information do we collect and store?

- 2.1 The School collects personal information:
  - (a) face-to-face when a person walks in to our reception office;
  - (b) online via our website;
  - (c) via email, post and phone; and
  - (d) at a school open day.
- 2.2 The kinds of personal information that the School may collect and hold include (but is not limited to) name, age, residential address, suburb, postcode, date of birth, phone number, email address, identification numbers, qualifications, employment information, health insurance details, marital status, bank account details, next of kin details, cultural information and images. We may also collect sensitive information from a person including a working with children check, health information or a police check.

## 3. What is a data breach?

- 3.1 Data breach means when this kind of personal information held by the School is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



- 3.2 Data breaches occur in a number of ways. Some examples include:
- (a) lost or stolen laptops, removable storage devices, or paper records containing personal information, for example the loss of a notebook containing client information;
  - (b) databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the School;
  - (c) paper records stolen from conference tables or insecure recycling or garbage bins;
  - (d) the School mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address; and
  - (e) an individual deceiving the School into improperly releasing the personal information of another person.

## 4. Response team

- 4.1 The Response Team is comprised of the members outlined in **Schedule A**.
- 4.2 It is the responsibility of the Team Leader (or if they are not available, the Deputy Team Leader) to implement the Plan or delegate responsibilities to ensure that the Plan is implemented.
- 4.3 The Response Team must work in consultation with the Principal in responding to a breach.

## STEP 1: CONTAIN THE BREACH AND DO A PRELIMINARY ASSESSMENT

### 5. Notify the Response Team

- 5.1 Any person that suspects a data breach may have occurred, or is likely to occur, must:
  - (a) use reasonable measures to contain the breach (if possible) as soon as practicable; and
  - (b) make a report to the Response Team using the Suspected Data Breach Report Form in **Schedule B** as soon as practicable.
- 5.2 Failure to comply with clause 5.1 may result in disciplinary action.

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



- 5.3 Once a report under clause 5.1(b) has been made, the Team Leader will implement immediate action to:
- (a) contain the breach to the extent possible (e.g. stop the unauthorised practice, recover the records, or shut down the system that was breached); and
  - (b) take steps to mitigate the harm an individual may suffer as a result of a breach (as necessary).

## 6. Preliminary assessment

- 6.1 The Team Leader will as soon as practicable make enquiries, and record the enquiries in writing, in relation to the following:
- (a) What personal information does the breach involve?
  - (b) What was the cause of the breach?
  - (c) What is the extent of the breach?
  - (d) What are the harms (to affected individuals) that could potentially be caused by the breach?
  - (e) How can the breach be contained?
- 6.2 Once the Team Leader has carried out the enquiries in clause 6.1, the Team Leader will inform the Response Team about the findings.

## STEP 2: EVALUATE THE RISKS ASSOCIATED WITH THE BREACH

### 7. Risk assessment

- 7.1 The Team Leader will complete the form in **Schedule C**.
- 7.2 Relevant factors to consider to assess the risks are:
- (a) The type of personal information involved.
  - (b) The context of the affected information and the breach.
  - (c) The cause and extent of the breach.
  - (d) The risk of serious harm to the affected individuals.

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



(e) The risk of other harms.

7.3 The Team Leader, in consultation with the Response Team and the Principal, will determine whether an eligible data breach has occurred.

## 8. Eligible data breach

8.1 An eligible data breach happens if:

- (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
- (b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates..
- (c) the entity has not been able to prevent the likely risk of serious harm with remedial action.

8.2 The Team Leader is required to complete the form in **Schedule D** and use this information to make a decision as to whether an eligible data breach has occurred or not.

8.3 If an eligible data breach has occurred, go to clause 9.

## STEP 3: NOTIFICATION

### 9. Notification if eligible data breach

9.1 Unless the exception under clause 9.3 applies, the Team Leader will notify:

- (a) the Office of the Australian Information Commissioner (**the OAIC**) as soon as practicable in circumstances where there are reasonable grounds to believe that a eligible data breach has happened or if directed to do so by the OAIC; and
- (b) all affected individuals either:
  - (i) directly (via email and/or post); or
  - (ii) if impracticable to notify all affected individuals directly, publish a statement on the School's website.

9.2 The notification to the OAIC in clause 9.1 must include:

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



- (a) the identity and contact details of the School;
- (b) a description of the eligible data breach that the School has reasonable grounds to believe has happened;
- (c) the kind or kinds of information concerned; and
- (d) recommendations about the steps that individuals should take in response to the eligible data breach.

## 9.3 Where:

- (a) there is unauthorised access to, disclosure or loss of information but the School takes action before it results in any serious harm to the affected individual; and
- (b) as a result of the action a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the individual,

then the unauthorised access or disclosure is deemed to have never been an eligible data breach.

## 10. How to notify?

- 10.1 In general, the recommended method of notification is direct – by phone, letter, email or in person – to the affected individuals.
- 10.2 Indirect notification, either by website information, posted notices, media, should generally only occur where direct notification could cause further harm (noting that website publication might constitute a data breach), is cost-prohibitive, or the contact information for affected individuals is not known.
- 10.3 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.
- 10.4 When providing notification to an affected individual or third parties, the notification should be given without any admission of liability.

## 11. Who else should be notified?

- 11.1 In addition to the affected individuals, it may also be appropriate to notify the following third parties:
  - (a) OAIC;

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



- (b) Police;
- (c) Insurers;
- (d) Credit card companies, financial institutions or credit reporting agencies; and/or
- (e) Professional or other regulatory bodies.

## STEP 4: REVIEW THE INCIDENT AND TAKE ACTION TO PREVENT FUTURE BREACHES

### 12. After action review

- 12.1 The School is committed to always improving its data security processes, particularly in circumstances where a data breach occurs.
- 12.2 Following a data breach, the School will implement measures to improve its data security processes in the future, such as conducting an investigation, updating policies and procedures, and providing staff training.

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



## SCHEDULE A – RESPONSE TEAM

Name	Position	Email address
Barbara Walsh	Team Leader	<a href="mailto:barbara.walsh@dsm.org.au">barbara.walsh@dsm.org.au</a>
Leon Gabler	Deputy Team Leader	<a href="mailto:leon.gabler@dsm.org.au">leon.gabler@dsm.org.au</a>

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



## SCHEDULE B – SUSPECTED DATA BREACH REPORT FORM

Name of person making report	
Date and time of suspected data breach	
What information was compromised (name, address, etc)	
Please provide the name of the person	
Please provide a detailed description of the incident	
Please list any actions that have been taken to contain the breach	
Please provide any further information	

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



## SCHEDULE C – EVALUATE THE RISKS ASSOCIATED WITH THE BREACH

<b>Consider the type of personal information involved</b>	
Is the information personal information or sensitive information?	
Does the type of information that has been compromised create a higher risk of harm?	
Who is affected by the breach?	
<b>Determine the context of the affected information and the breach</b>	
What is the context of the personal information involved?	
What parties have gained unauthorised access to the affected information?	
Have there been other breaches that could have a cumulative effect?	
How could the personal information be used?	
<b>Establish the cause and extent of the breach</b>	
Is there a risk of ongoing breaches or further exposure of the information?	
Is there evidence of theft?	

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?	
What was the source of the breach?	
Has the personal information been recovered?	
What steps have already been taken to mitigate the harm?	
Is this a systemic problem or an isolated incident?	
How many individuals are affected by the breach?	
<b>Assess the risk of harm to the affected individuals</b>	
Who is the recipient of the information?	
What harm to individuals could result from the breach?	
<b>Assess the risk of other harms</b>	
Other possible harms, including to the agency or organisation that suffered breach	
Other possible harms, including to the agency or organisation that suffered the breach	

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



## SCHEDULE D – ELIGIBLE DATA BREACH

An eligible data breach happens if:

- there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
- the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

The determination as to what is ‘serious harm’ is an objective ‘reasonable person’ test. That is, whether a reasonable person would conclude that access to or disclosure of the personal information would be likely to result in serious harm to any of the individuals to whom the information relates. “Serious harm” is to be broadly construed and may include physical, emotional, economic and financial harm as well as reputational damage.

To determine whether a reasonable person would conclude that an access to, or disclosure of, information would be likely to or would not be likely to result in serious harm to any of the individual to whom the information relates, regard must be given to the factors outlined below.

Once a report is made to the Response Team relating to a data breach, the Team Leader is required to complete this form in order to consider whether an eligible data breach has occurred or not.

Factor	Response / Relevant information considered
The kind or kinds of information	
The sensitivity of the information	
Whether the information is protected by one or more security measures	

# DSM Data Breach Response Plan

Deutsche Schule Melbourne Inc, ABN 52 936 931 854



If the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome	
The persons, or the kinds of persons, who have obtained, or who could obtain, the information	
The nature of the harm	
Any other relevant matters	

Created, June 2019