FRÖBEL
Competence for Children

DATA BREACH RESPONSE PLAN

PURPOSE

The purpose of this policy is to detail the Priority of Access Guidelines as specified by the Australian Government.

POLICY

This data breach response plan (response plan) sets out procedures and clear lines of authority for FROEBEL staff in the event the FROEBEL experiences a data breach (or suspects that a data breach has occurred).

PROCEDURES

A data breach occurs when personal information is accessed or disclosed without authorisation or lost. Under the Notifiable Data Breaches (NDB) scheme FROEBEL must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) (as regulator) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances. For example, personal information may include:

- an individual's name, signature, address, phone number or date of birth
- sensitive information
- credit information
- employee record information
- photographs
- internet protocol (IP) addresses
- voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique)
- location information from a mobile device (because it can reveal user activity patterns and habits).

The Privacy Act 1988 doesn't cover the personal information of someone who has died.

Sensitive information is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or associations

- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information
- some aspects of biometric information
- Generally, sensitive information has a higher level of privacy protection than other personal information.

For good privacy practice purposes, this response plan covers any instances of unauthorised use, modification, interference with or loss of personal information held by FROEBEL. 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 and entities.

This response plan is intended to enable FROEBEL to contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals and to comply with the NDB scheme. The actions in the first 24 hours after discovering a data breach are crucial to the success of the response.

The plan 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 FROEBEL to respond to a data breach.

Responding to a data breach

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. Depending on the nature of the breach, the response team may need to include additional staff or external experts, for example an IT specialist/data forensics expert or external legal advisors. The Managing Director will put together the most suitable and effective response team on a case-by-case basis as required.

When responding to a data breach officers should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. At all times, officers should consider what remedial action can be taken to reduce any potential harm to individuals.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

STEP 1: Identify the breach

A suspected data breach may be discovered by a FROEBEL staff member or contractor or FROEBEL may be otherwise alerted (eg. by a member of the public or the media).

If you become aware of, or are notified of a data breach, immediately notify the Managing Director of the suspected data breach. A data breach suspected by the Managing Director may be reported directly to the FROEBEL headquarters in Berlin/Germany.

Record and advise the Managing Director of the following (if known at the time of the report):

- the time and date the suspected breach was discovered,
- the type of personal information involved,
- the cause and extent of the breach, and
- the context of the affected information and the breach.

STEP 2: Contain the breach and notify the Chief Privacy Officer (Director)

The Managing Director should seek to understand, assess and contain the breach. As soon as the Managing Director is made aware of the breach or suspected breach, the Managing Director should seek all the facts to enable an initial assessment of whether a data breach has or may have occurred and the seriousness of the data breach or suspected data breach. This should be done within the first hour of being so made aware.

The Managing Director should co-ordinate any immediate action required to contain the breach. Depending on the breach, this may include contacting incorrect recipients requesting them to delete the email or requesting information be removed from a website.

STEP 3: Assess the risks for individuals associated with the breach and make a record

It is the Managing Director's role to determine whether the breach constitutes a Notifiable Data Breach. The Managing Director should initially assess the data breach, which may involve asking for further information or documentation from the person who reported the breach or the FROEBEL staff member who identified the breach.

Collection of the following information about the breach should form part of that assessment by the Managing Director:

- 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.

Following that assessment, the Managing Director must decide whether any further action is required to contain the breach, including but not limited to the following:

- recommending to IT to implement certain response measures
- alerting building security if necessary
- advising the Board of Directors of the incident.

Record-Keeping

The Managing Director co-ordinates the record keeping for each data breach in the CammsRisk register, regardless of whether the breach amounts to a Notifiable Data Breach. The log must include the reasons why the Managing Director did or did not classify the matter as a Notifiable Data Breach.

Informing the Board of Directors

The Managing Director must inform the Board of Directors as soon as possible after being made aware of a suspected or actual data breach and must provide ongoing updates on key developments. The Managing Director should consult the Board of Directors in relation to any breach that may amount to a Notifiable Data Breach.

STEP 4: Consider breach notification and calling data breach response team

The Managing Director is to use discretion in deciding whether to escalate to a broader response team.

On each occasion of a data breach, the Managing Director must consider whether to convene a Data Breach Response Team (response team).

Some data breaches may be comparatively minor, and able to be dealt with easily without action from a response team. For example, a FROEBEL staff member 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 successfully recalled (only relates to internal emails), or if the staff member can contact the recipient and obtain an assurance that the recipient has deleted the email, it may be that there is no utility in escalating the issue to the response team.

The Managing Director should use their discretion in determining whether a data breach or suspected data breach requires escalation to the response team. The decision to escalate to the response team should be made immediately following the Managing Director's assessment about the data breach after the collation of relevant material.

In making that decision the Managing Director 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 any of the affected individual(s)?

- Does the breach or suspected breach indicate a systemic problem in FROEBEL processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

Once the Managing Director decides that a data breach or suspected data breach requires escalation to the response team, they should co-ordinate the convening of the response team, ideally on the same working day. The response team should be convened with members meeting in person or via secure teleconference facilities.

The checklist below sets out the steps that the response team will take:

- Conduct initial investigation, and collect information about the breach promptly.
- 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.
- Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.
- Consider whether the breach is an eligible data breach under the NDB scheme

It is the Managing Director's role to determine whether the breach constitutes a notifiable data breach. This decision may be informed by the views of the response team. If the Managing Director determines that the data breach is an eligible data breach, they and the response team must co-ordinate notifications required under the NDB scheme. If there are reasonable grounds to believe an eligible data breach has occurred, FROEBEL must promptly notify any individual at risk of serious harm and notify the Australian Information Commissioner using the NDB form on the OAIC's website.

An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an organisation or agency (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The organisation or agency has been unable to prevent the likely risk of serious harm with remedial action.

Consider whether others should be notified

The Managing Director and/or response team should consider whether others should be notified, including:

- the Australian Cyber Security Centre (ACSC), police/law enforcement, or
- other agencies or organisations that:
    - may be affected by the breach, or
    - can assist in containing the breach, or
    - can assist individuals affected by breach, or

- where FROEBEL is contractually required or required under the terms of an MOU or similar obligation to notify specific parties.

STEP 5: Review the incident and take action to prevent future breaches

Following data breaches, in cases where the Managing Director has not convened the response team, they will undertake a post breach review and draft a report outlining the cause of the breach, implementing any strategies to identify and address any weaknesses in data handling that may have contributed to the breach, and making appropriate changes to policies and procedures if necessary.

In cases where the Managing Director has convened the response team, the response team should conduct a post-breach review (and draft a report) assessing FROEBEL's response to the breach and the effectiveness of this data breach response plan. The review should consider:

- The full investigation of the cause of the breach.
- Implementing a strategy to identify and address any weaknesses in data handling that contributed to the breach
- Updating data breach response plan if necessary.
- Making appropriate changes to policies and procedures if necessary.
- Revising staff training practices if necessary.
- Considering the option of an audit to ensure necessary outcomes are affected.
- Considering whether the response team needs other expertise
- The preservation of evidence to determine the cause of the breach or allowing FROEBEL to take appropriate corrective action.
- A communications or media strategy to manage public expectations and media interest.

The post-breach review report to be drafted by response team members should outline the above considerations, identify any weaknesses in this data breach response plan and include recommendations for revisions or staff training as needed. The response team should report the results of the post-breach review (and hand up the post-breach review report) to the Board of Directors.

FROEBEL's Data Breach Response Check List

Step 1: Identify the breach

Record and advise the Managing Director of the following:

- the time and date the suspected breach was discovered,
- the type of personal information involved,
- the cause and extent of the breach, and
- the context of the affected information and the breach.

Step 2: Contain the breach (Managing Director)

- Understand and assess the data breach, or suspected data breach
- Co-ordinate any action required to contain the data breach

- Notify the Chief Privacy Officer about the data breach.

Step 3: Assess the risks for individuals associated with the breach (Managing Director)

- Conduct initial investigation to establish the cause and extent of the breach.
- Assess priorities and risks based on what is known.
- Notify FROEBEL Executive about the data breach.
- Keep appropriate records of the suspected breach including any action taken.

Step 4: Consider breach notification and convene response team

- Determine who needs to be made aware of the breach at this preliminary stage.
- Determine whether and how to notify affected individuals.
- Determine whether to escalate the data breach to the response team.
- Convene the response team, if necessary.
- Determine whether the breach is an eligible data breach under the NDB scheme.
- Notify the AIC of the NDB, if necessary.

Step 5: Review the incident and take action to prevent future breaches

- Fully investigate the cause of the breach.
- Implement a strategy to identify and address any weaknesses in FROEBEL data handling.
- Conduct a post-breach review and report to FROEBEL Executive on outcomes and recommendations.

SOURCES AND FURTHER READING

- Office of the Australian Information Commissioner: Data breach preparation - A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) https://www.oaic.gov.au/__data/assets/pdf_file/0017/1691/data-breach-preparation-and-response.pdf
- Privacy Act 1988 (Cth) http://www5.austlii.edu.au/au/legis/cth/consol_act/pa1988108/

ASSOCIATED POLICIES

- Privacy and Confidentiality

POLICY REVIEW

- The Approved Provider will review this policy every 12 months.
- The Approved Provider and Centre Director ensure that at all times all FROEBEL staff maintain and implement this policy and its procedures.

- **Last review**: 10.01.2024
- **Next review**: 10.01.2025