SKATE VICTORIA INC

Data Breach Plan

Version 2 - Sep 2023

Contents

Acknowledgement

OF COUNTRY

Skate Victoria acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea, and community. We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

OF DIVERSITY AND INCLUSION

Skate Victoria recognises that inclusion is about making sure our sport reflects the diversity of all participants and are committed to providing a safe, welcoming, and respectful culture where everyone feels welcome and accepted regardless of age, gender, ability, socio economic status or cultural, ethnic, or religious background.

OF SAFE ENVIRONMENTS

Skate Victoria is committed to the safety and well-being of all children and young people who participate in our sport or access our services. We support the rights of the child and will always act to ensure that a child-safe environment is maintained.

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 is no single method of responding to a data breach.

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

Committees should refer to the checklist below and to the Office of the Australian Information Commissioner's *Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*.

www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

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

Identify the Breach

If you become aware of, or are notified of a data breach the committee. A data breach suspected by a member of the committee may be reported directly to the Chief Executive Officer.

Record and advise your committee 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.

Contain the Breach

The committee should seek to understand, assess and contain the breach. As soon the committee is made aware of the breach or suspected breach, they 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 committee 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.

Notification of the breach should include the following information:

- a description of the breach or suspected breach,
- the action taken by the committee to address the breach or suspected breach,
- the outcome of that action,
- a view as to the seriousness of the breach, and
- a view as to whether any further action is required.

Assess the Risks for Individuals Associated with the Breach and Make a Record

It is the committee's role to determine whether the breach constitutes a Notifiable Data Breach, they should initially assess the data breach, which may involve asking for further information or documentation.

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

- 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 Committeee must decide whether any further action is required to contain the breach.

Review the Incident and Take Action to Prevent Future Breaches

Following data breaches, 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.

Testing this Plan

Committees should test this plan with a hypothetical data breach at least annually to ensure that it is effective.

References and Acknowledgements

Australian Government

Office of the Australian Information Commissioner

www.oaic.gov.au/about-us/our-corporate-information/key-documents/data-breach-response-plan

Document Revision History

March 2022	Data Breach Plan	Created
September 2023	Cover and Contents Page	Updated

SKATE VICTORIA INC