ROYAL ACADEMY OF DANCE

Document	**Governance of Data Policy**
Effective Date	01/10/22
Review Date	End of each calendar year
Authorized by	National Director
Associated Documents	Privacy Policy
Responsible Officer	All RAD Employees

1. STATEMENT OF PRINCIPLE

The RAD is committed to ensuring an efficient, effective, and acceptable use of data. It is responsible for ensuring no significant harm is caused to individuals because of a data breach arising from the RAD's collection and storing of data.

The current policy adopts the principles and processes outlined in;

- ISO/IEC 38505-1 Information technology – Governance of IT – Governance of data
- Office of the Australian Information Commissioner – Data breach preparation and response

2. SCOPE

This policy sets out the process for identifying and reporting breaches of the RAD data.

3. DEFINITIONS

The RAD means, the Royal Academy of Dance Australia

National Director, means the National Director of the RAD

Commissioner means the Office of the Australian Information Commissioner

Data breach means the unauthorised access or disclosure of personal information, or loss of personal information.

Eligible Data Breach means the unauthorised access or disclosure of personal information, or loss of personal information in circumstances where this is likely to occur, that is likely to result in serious harm to any of the individuals to whom the information relates (see s 26WE(2) of the Privacy Act). Please see clause 6 for further information.

Likely to occur means the risk of serious harm to an individual is more probable than not (rather than possible).

NDB scheme is the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act.

Serious harm means harm to physical or mental well-being, financial loss, or damage to reputation as a result of personal information involved in a data breach.

Privacy Act is the Privacy Act 1988 (Cth).

Personal information is defined in s 6(1) of the Privacy Act, as information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Reasonable person means a person in THE RAD's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach. In general, entities are not expected to make external enquiries about the circumstances of each individual whose information is involved in the breach.

Remedial action is the steps that an entity may take to prevent the likelihood of serious harm occurring for any individuals whose personal information is involved in an Eligible Data Breach.

Sensitive information is defined in s 6(1) of the Privacy Act to include personal information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. Sensitive information also includes all health information, genetic information, biometric information that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates.

4. NOTIFIABLE DATA BREACHES SCHEME (NDB)

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.

Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

Examples of harm include:

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family violence
- physical harm or intimidation.

A data breach can also negatively impact an entity's reputation for privacy protection, and as a result undercut an entity's commercial interests. If an entity is perceived to be handling personal information contrary to community expectations, individuals may seek out alternative products and services.

An entity can reduce the reputational impact of a data breach by effectively minimising the risk of harm to affected individuals, and by demonstrating accountability in their data breach response. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables individuals to take steps to reduce their risk of harm. It also demonstrates that an entity takes their responsibility to protect personal information seriously, which is integral to building and maintaining trust in an entity's personal information handling capability.

The NDB became law on 22 February 2018. As a not-for-profit with greater than $3 million annual turnover, THE RAD is subject to the law.

5. ELIGIBLE DATA BREACH

An Eligible Data Breach arises when the following three criteria are satisfied:

a) there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, held by the RAD.

b) this is likely to result in serious harm to one or more individuals, and

c) the RAD has not been able to prevent the likely risk of serious harm with remedial action.

6. PROCESS

All RAD employees are responsible for reporting suspected Eligible Data Breaches to the National Director. Upon learning of a suspected data breach the National Director, or their delegate, shall:

STEP 1 Determine if there has been a data breach

STEP 2 Determine if serious harm is likely

STEP 3 Put in place measures to prevent serious harm with remedial action.

STEP 4 Where appropriate, notify individuals at risk of serious harm, RAD Global, and the Commissioner.

STEP 5 Ensure records of all data breaches, Eligible or otherwise are kept.

STEP 6 Review actions following a breach

7. STEP 1: DETERMINE IF THERE HAS BEEN A DATA BREACH

The first step in deciding whether an Eligible Data Breach has occurred involves considering whether there has been a data breach; that is, unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information (s 26WE(2)). The Privacy Act 1988 (Cth) (Privacy Act) does not define these terms. Unauthorised access of personal information occurs when:

a) personal information held by the RAD is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

b) There is intentional or unintentional disclosure of personal information to others outside the entity in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee.

c) There is accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or disclosure. Under the NDB scheme, if personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no Eligible Data Breach (s 26WE(2)(b)(ii)).

8. STEP 2: DETERMINE IF SERIOUS HARM IS LIKELY

The second step in deciding whether an Eligible Data Breach has occurred involves deciding whether, from the perspective of a Reasonable Person, the data breach would be likely to result in serious harm to an individual whose personal information was part of the data breach.

Entities should assess the risk of Serious Harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm. When considering whether Serious Harm has occurred the RAD shall consider:

a) the kind or kinds of information

b) the sensitivity of the information

c) whether the information is protected by one or more security measures and the likelihood that any of those security measures could be overcome

d) the persons, or the kinds of persons, who have obtained, or who could obtain, the information

e) if a security technology or methodology:

    a. was used in relation to the information, and;
    b. was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information

f) the likelihood that the persons who have obtained, or who could obtain, the information;

    a. have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;

    b. have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology

g) the nature of the harm. The RAD will consider the broad range of potential kinds of harms that may follow a data breach. Examples may include:

    a. identity theft

    b. significant financial loss by the individual

    c. threats to an individual's physical safety

    d. loss of business or employment opportunities

    e. humiliation, damage to reputation or relationships

    f. workplace or social bullying or marginalization.

h) whose personal information was involved in the breach.

i) the number of individuals involved.

j) whether the circumstances of the data breach affect the sensitivity of the personal information.

k) the length of time the information has been accessible.

l) whether the information has been adequately encrypted, anonymized, or otherwise not easily accessible.

m) any other relevant matters.

10. STEP 3: PREVENTING SERIOUS HARM WITH REMEDIAL ACTION

The RAD will take positive steps to address a data breach in a timely manner. Remedial action such that the data breach would not be likely to result in serious harm will remove the requirement to notify the Commissioner. For breaches where information is lost, the remedial action is adequate if it prevents unauthorised access to, or disclosure of personal information.

If the remedial action prevents the likelihood of serious harm to some individuals within a larger group of individuals whose information was compromised in a data breach, notification to those individuals for whom harm has been prevented is not required.

11. STEP 4: NOTIFICATION

When the RAD is aware of Reasonable grounds to believe an Eligible Data Breach has occurred it will:

a) promptly notify individuals at likely risk of serious harm,

b) promptly notify the RAD Global, and

c) notify the Commissioner as soon as practicable through a statement about the Eligible Data Breach.

The notification to affected individuals and the Commissioner must include the following information:

a) the identity and contact details of the organization

b) a description of the data breach

c) the kinds of information concerned and;

d) recommendations about the steps individuals should take in response to the data breach.

The notification to the Commissioner should be made using the **OAIC's Notifiable Data Breach form.** (Office of Australian Information Commission)

12. STEP 5: RECORD OF DATA BREACH

The RAD will keep a record of data breach incidents, including those that are not notifiable. This will assist the RAD to ensure it has met regulatory requirements.

13. STEP 6: REVIEW FOLLOWING A BREACH

Evaluating how a data breach occurred, and the success of the response, will help the RAD improve its data handling and data breach management. The RAD shall:

a) review all data handling procedures that contributed to a breach within 30 days of the breach, and

b) implement a system for a post-breach assessment of its response to the data breach and the effectiveness of its actions.