# Wyndham Community and Education Centre Inc.
# Policy and Procedure

| | |
|---|---|
| Policy name | **Data Breach Response Policy & Procedure** |
| Responsible person | Privacy Officer, Board of Governance, CEO |
| Staff involved | All |
| Review dates | 2019 |
| Related documents | **Legislation**: Privacy Act 1988 (Cth), Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth), Information Privacy Act 2000 (Vic), Health Records Act 2001 (Vic), Privacy and Data Protection Act 2014 (Vic), Freedom of Information Act 1982 (Cth), Charter of Human Rights & Responsibilities Act 2006 (Vic), Public Records Act 1973 (Vic), Surveillance Devices Act 1999 (Vic), Spam Act 2003 (Cth), Disability Act 2006 (Vic), Children, Youth and Families Act 2005 (Vic)<br>**Policies:** Privacy Policy & Procedure, Student Selection, Enrolment & Induction (Foundation Skills) Policy & Procedure, Student Selection, Enrolment & Induction (VET) Policy & Procedure, Student Selection, Enrolment & Induction (VCAL) Policy & Procedure, Record Management & Record Keeping Policy & Procedure, Child Safe Policy & Procedure, Complaints and Appeals Policy & Procedure, mandatory Reporting Policy & Procedure, National Police Checks Policy & Procedure, Cyberbullying Policy & Procedure, Duty of Care Policy & Procedure (Under-18s), Social Media Policy & Procedure,<br>**Other:** Privacy & Your Rights Tri-fold, Privacy Agreement for Staff & Volunteers, Request to view my own file Form, Enrolment Form, Wyndham CEC Website Privacy Statement, Australian Privacy Principles (APPs), Information Privacy principles (IPPs), Rules of Association, 2018 SF VET Funding Contract, Victorian VET Student Statistical Collection Guidelines 2018, DSS Settlement Services Grant Agreement, Notifiable Data Breach Scheme, DHHS Service Agreement, Victorian Protective Data Security Framework (VPDSF), OAIC Data Breach Preparation and Response Guide - oaic.gov.au, Privacy Guide (Justice Connect), Data Breach Incident Reporting Form, Data Breach Incident Reporting Form, Department of Health Information Management Security Incident Response Plan |

## Policy Context

Wyndham Community and Education Centre Incorporated *(Association Number A0002509M),* is a not-for-profit association established in 1974 and governed by a Board of Governance, comprised of elected community members and stakeholders.

Wyndham Community and Education Centre (Wyndham CEC) offers a range of community and education programs and services to members of the local Wyndham community and surrounds. Many of these programs and services are government funded.

Wyndham CEC is an entity governed by the *Privacy Act 1988 (Cth).*

## Policy

Wyndham CEC collects, uses and stores information disclosed by individuals it interacts with. Some of this information is classified as personal information under privacy laws and may include sensitive personal information and health information.

The data collected is used for planning, management and monitoring of Wyndham CEC's services and program activities and includes staff, students and clients of Wyndham CEC as well as other organisations Wyndham CEC interacts with. Personal information will only be used or disclosed for the primary purpose for which it was collected for example, to meet funding and performance reporting obligations.

Information at Wyndham CEC is held in many forms such as student records, reports, personnel records, paper files, and computerised databases and documents. It may be transmitted in many ways including by hand, by courier, or electronically using various communications technologies. Information may be transmitted through systems controlled by the Federal Government, Victorian Government or systems controlled by external parties.

The principles underlying the need for information security apply to all information irrespective of the media on which it is held.

This policy applies to all persons employed at Wyndham CEC (including contractors, students, volunteers and users of the centre).

This policy also applies to external organisations and their personnel who have been granted access to Wyndham CEC Information and Communication Technology (ICT) infrastructure, services and data.

The scope of the policy includes Wyndham CEC data held in any format or medium (paper based or electronic) that has been designated as a non-public document. The policy does not apply to information that has been classified fit for public distribution.

The policy covers data collection within Wyndham CEC. It includes collections of client, corporate, financial and workforce information. For the purpose of this policy, data collection includes both operational data collections and data repositories.

Depending on the type and extent of a **data breach**, management of public relations may be required, including coordinating the timing, content and method of public announcements and similar activities.

This policy outlines the immediate responses of Wyndham CEC in the event of a data breach.

Wyndham CEC has a **Privacy Officer** who can be contacted via email, mail or phone:
privacy@wyndhamcec.org.au or 20 Synnot Street, Werribee VIC 3030/ 97424013.

**The Australian Privacy Principles (APPs)**

The *Privacy Act 1988 (Cth)* contains 13 APPs that detail an organisations obligations for the management of personal information. The APPs ensure that risks are reduced

or removed when handling personal information. Compliance with the APPs forms best practice and will assist organisations to avoid a data breach. For more on the APPs see Wyndham CEC's *Privacy Policy and Procedure* (staff & volunteers / students & clients).

## 1. What is a data breach?

Since the introduction of the *Australian Privacy Principles* (APPs) under the *Privacy Act 1988 (Cth),* organisations must take reasonable steps to prevent the **loss**, **unauthorised access**, **modification** or **disclosure** of personal information it collects and stores.

A data breach is defined as unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information whether accidently or intentionally.

Personal information is information about an identified individual, or an individual who is reasonably identifiable. Personal information can also be classified as sensitive information and health information. Wyndham CEC has key obligations when dealing with privacy to keep personal information secure, accurate and up-to-date.

Sensitive information includes (but is not limited to): health information; documents used for identity fraud such as Medicare card, Passport, driver licence; financial information.

## 2. Types of Data Breaches

### a. Unauthorised access

Unauthorised access of personal information occurs when personal information that Wyndham CEC holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of Wyndham CEC, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

### b. Unauthorised disclosure

Unauthorised disclosure occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside Wyndham CEC, and releases that information from effective control in a way that is not permitted by the *Privacy Act 1988 (Cth)*. This includes an unauthorised disclosure by an employee of Wyndham CEC.

### c. Loss

Loss refers to the accidental or inadvertent loss of personal information held by Wyndham CEC, in circumstances where is it is likely to result in unauthorised access or disclosure.

### 3. Notifiable Data Breaches scheme

The Notifiable Data Breaches (NDB) scheme under Part IIIC of the *Privacy Act 1988 (Cth),* establishes requirements for entities in responding to data breaches.

Entities have data breach notification obligations when it has reasonable grounds to believe that it has experienced a data breach in which there is unauthorised access or disclosure or loss of personal information and that the data breach is likely to result in serious harm to any individual whose personal information is involved in the breach. Examples of serious harm include (but are not limited to):

- financial fraud
- family violence
- identity theft
- emotional/ psychological harm
- reputational harm

The Notifiable Data Breaches (NDB) scheme requires regulated entities to notify particular individuals and the Australian Information Commissioner about **eligible data breaches**.

An **eligible data breach** arises when the following three criteria are satisfied:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds
- this is likely to result in serious harm to one or more individuals, and
- Wyndham CEC has not been able to prevent the likely risk of serious harm with remedial action.

There may be other obligations outside of the *Privacy Act 1988 (Cth)* that relate to personal information protection and responding to data breaches. These include but are not limited to:

- Australian Taxation Office
- Department of Health & Human Services
- Regulatory bodies
- Police
- Insurance providers
- Financial providers

### 4. Data Breach Response – four key steps

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.

**Step 1: Contain** the data breach to prevent further compromise of personal information. In the event of a breach, the person who discovers the breach should immediately initiate a process of containment by taking whatever steps possible to immediately contain the breach. For example:

- stop the unauthorised practice
- recover any records
- shut-down the system that was breached. If it is not practical to shut down the system, then revoke or change the account privileges or block access from the unauthorised person
- encryption making notification unnecessary
- recalling email

The person who discovers the breach must collect information about the breach promptly and the details must be recorded in Part A of the **Data Breach Incident Reporting Form** (Appendix 1).

They must also make an initial assessment using the **Data Breach Impact Severity Ratings Form** (Appendix 2).

The **Privacy Officer** must be notified immediately of the breach and be provided with the *Data Breach Incident Reporting Form* with Part A completed.

**Step 2: Assess** the data breach by gathering the facts and evaluating the risks including potential harm to affected individuals and where possible taking action to remediate risk of harm. This step needs to happen quickly and a decision made to notify should be made as soon as possible.

An assessment should be a three-step process: **initiate; investigate;** and**, evaluate.**

The **Privacy Officer** is responsible for undertaking a risk assessment and evaluating the risks to individuals associated with the breach as well as the risks for Wyndham CEC. In undertaking a risk assessment the Privacy Officer should use the Data Breach Impact
Severity Ratings Form (Appendix 2) to determine the impact severity of the data breach.

The **Privacy Officer** will need to determine the risk of harm to the affected individuals and determine the risk of harm to Wyndham CEC. Some examples of possible harm to Wyndham CEC include:

- the loss of public trust in the agency or particular program
- the loss of assets, for example, stolen computers or storage devices
- financial exposure, for example, if bank account details are compromised
- regulatory penalties or legal liability to any third party.

After completing the *Data Breach Incident Reporting Form* the **Privacy Officer** must decide whether further investigation into the data breach is required and document how this will be undertaken, where applicable.

Further actions may include interviews (or further interviews) with staff involved and/or affected, or the request of further investigation by appropriate Wyndham CEC staff into system failures or ICT security issues.

To assess the risks, the following factors should be considered:

- the type of personal information involved e.g. Medicare numbers, health information, phone numbers and who is affected by the breach
- the context of the affected information and breach e.g. how was the information used
- the cause and extent of the breach e.g. what was the source of the breach? Is there a risk of further exposure of the information? Is this a recurring problem of the system?
- the risk of serious harm to the affected individuals and the risk of other harms e.g. what harm occurred as a result of the breach, such as, financial loss or threat to physical health.

Wyndham CEC will take all reasonable steps to complete the assessment within a maximum of 30 calendar days after the day it becomes aware of an eligible data breach bearing in mind that for serious harm to an individual to be avoided, a shorter timeframe may be recommended.

Wyndham CEC may not need to notify if it takes remedial action in a timely manner and has mitigated the likelihood of serious harm to an individual.

**Step 3: Notify** individuals affected and the Commissioner if required as soon as practicable in order to mitigate harm.

The **Privacy Officer** must consider the particular circumstances of each breach and determine, using the Data Breach Impact Severity Ratings Form (Appendix 2), the level of notification within Wyndham CEC.

Consideration also needs to be given on whether notification is provided to any affected individuals and/or the Australian Information Commissioner. In some cases, if there is a high level risk of serious harm to individuals, it may be appropriate to notify them immediately.

The **Privacy Officer**, in conjunction with the **Chief Executive Officer** (CEO), should assess:

- whether or not to notify individuals and if so when and how the notification should occur, who should make the notification, and who should be notified
- whether the data breach is classified as an 'eligible data breach'
- what information should be included in the notification

- who else should be notified such as the police/law enforcement, other agencies or organisations affected by the breach, parties under the terms of an agreement such as a Memorandum of Understanding (MoU) or contract.

The **Privacy Officer** is responsible for completing Part B of the Data Breach Incident Reporting Form and provide a report for consideration, to the required person(s), as stipulated in the Data Breach Severity Ratings Form. The report should provide a recommendation of either no further action necessary or provide details to any further action(s) and the reasoning for the recommendations.

All staff should report incidents of suspected misconduct related to data as soon as practicable to the **Privacy Officer**. These instances must also be escalated, as appropriate to the **CEO**.

**Step 4: Review** the incident and consider what preventative actions can be taken.

The **Privacy Officer** must ensure that the cause of the breach has been fully investigated and that the **CEO** has been briefed on outcomes and recommendations, as appropriate.

At a minimum, amendments to policies and procedures should be made where necessary and staff training should be undertaken where deemed appropriate. A debriefing session should be held with relevant staff to assess the response to the breach and to ensure any necessary recommendations are allocated and actioned appropriately.

The significance of the breach should be reviewed as to whether it was an isolated event or a recurring breach. A prevention plan should include:

- a security audit of both physical and technical security
- a review of employee selection and training practices
- a review of policies and procedures to reflect the lessons learned from the investigation
- staff training in responding to data breaches effectively.

Wyndham CEC will audit its data security systems annually through the Data Breach Response Plan.

## 5. Data breaches involving more than one entity

The NDB scheme recognises that organisations such as Wyndham CEC may hold information jointly with another entity. For example one may have physical possession of the information and the other legal control or ownership.

In such cases, an eligible data breach of one will be deemed an eligible data breach of the other and both will have obligations under the NDB scheme. Compliance will

only need to be undertaken by one entity and there is flexibility under the NDB for both to decide the most relevant entity to take necessary steps.

The OAIC recommendation is that the entity with the most direct relationship with the individuals affected by the data breach should carry out the notification. Wyndham CEC will follow this recommendation when allocating responsibility in such an instance.

An example of when an entity holds joint information includes:

- Outsourcing arrangements
- Commonwealth contracts
- Subcontracting arrangements

## 6. Forms for Reporting a Data Breach

### a. Data Breach Incident Reporting Form

A Data Breach Incident Reporting Form (Appendix 1) should be completed by Wyndham CEC staff in all instances of a data breach or suspected data breach.

The form is comprised of two parts, **Part A** and **B**.

**Part A** is to be completed immediately, by the person who discovers or suspects the breach. The following details must be recorded:

- the date, time, duration and location of the breach
- how the breach was discovered or is suspected
- description of the incident and the type of data involved in the breach
- the cause and extent of the breach
- other staff members that either witnessed the event or were notified at the time of the incident
- an initial breach impact severity rating.

The **Privacy Officer** must complete **Part B** of the Data Breach Incident Reporting Form by providing the following details:

- details of who is affected by the data breach and the estimated number of individuals affected
- a description of the immediate actions taken to contain the breach
- details of anyone else notified of the incident and, if so, how and when they were notified
- whether any evidence has been preserved
- if any further investigation is considered necessary
- if any steps have been taken to prevent the data breach from occurring again.

### b. Data Breach Impact Severity Ratings Form

The Data Breach Impact Severity Ratings Form (Appendix 2) provides a standardised approach for assessing the severity of a data breach and outlines the reporting requirements for data breach notification. The form also helps in determining if an **eligible data breach** has occurred. Staff are required to make an initial assessment using the Data Breach Impact Severity Ratings Form and to notify the **Privacy Officer** of the breach in accordance with this form.

The impact severity rating of a data breach can range from negligible to very high. A rating should be considered against each of the categories below:

- risk to individual's safety
- distress caused to any party or damage to any party's standing or reputation
- unauthorised release of personally or commercially sensitive data to third parties
- threat to Wyndham CEC or third party systems, or capacity to deliver services
- financial loss to Wyndham CEC or liability to a third party

### c. Data Breach Response Team

Wyndham CEC's data breach response team include the **Privacy Officer,** the **Marketing & Technology Officer** (MTC) and the **CEO**.

All instances of a data breach will be tabled at senior management meetings.

### d. Responding to a privacy breach or complaint

Individuals have the right to complain if they believe a breach of their personal information has taken place. As per the *Privacy Policy & Procedure*, Wyndham CEC will respond to a privacy complaint within 30 days.

## 7. Data Retention

Once a data breach has been investigated, any related documentation must be kept and stored by the **Privacy Officer** as required.

## APPENDIX 1: DATA BREACH INCIDENT REPORTING FORM (PART A)

| DATA BREACH INCIDENT REPORTING FORM | |
|---|---|
| **PART A - Information to be completed by staff reporting the incident** | |
| **Full Name** | |
| **Position Title and Service Unit** | |
| **Contact Information** | |
| **Details of the Incident** | |
| **Date, time, duration and location of the breach.** | |
| **How was the breach discovered?** | |
| **Description of the incident, including what Wyndham CEC systems may be affected.** | |
| **Cause of the breach (if known).** | |
| **Was any other staff member notified or was a witness to the incident?** | |
| **DATA BREACH IMPACT SEVERITY RATING (refer to Appendix 2).** | |
| **1. Negligible 2. Low 3. Medium 4. High 5. Very High**<br>**Provide reasoning for the allocation of the impact rating:** | |
| **Signature:** **Date:** | |

## APPENDIX 1: DATA BREACH INCIDENT REPORTING FORM (PART B)

| DATA BREACH INCIDENT REPORTING FORM | |
|---|---|
| **PART B - Information to be completed by Privacy Officer** | |
| **Full Name** | |
| **Position Title and Service Unit** | |
| **Contact Information** | |
| **Do you agree with the Data Breach Impact Severity Rating?**<br>**YES NO (circle answer)**<br>**If no, please document the amended rating and reasoning:** | |
| **Details of the Incident** | |
| **Who does the data breach affect?**<br>**(e.g. staff, clients, general public, government agencies, any third party).** | |
| **Estimated number of individuals affected.** | |
| **Description of immediate actions taken to contain the data breach.** | |
| **Was anyone else notified of the data breach? Contact details and when.** | |
| **Cause and estimated cost of the data breach (if known).** | |
| **Has evidence been preserved? Please specify.** | |
| **Is further investigation considered necessary and how will this be undertaken?** | |
| **Have steps been taken to prevent the breach from occurring again?** | |
| **Signature:** **Date:** | |

**APPENDIX 2 (this has been adapted from *Department of Health Victoria, Information Management Security Incident Response Plan)***

| DATA BREACH IMPACT SEVERITY RATINGS FORM | | | | | |
|---|---|---|---|---|---|
| **Impact Type** | **Lowest** ← | | **Severity** | → | **Highest** |
| **Impact Severity** | **1. NEGLIGIBLE** | **2. LOW** | **3. MEDIUM** | **4. HIGH** | **5. VERY HIGH** |
| **Risk to individual safety due to unauthorised access or disclosure of classified information** | **No injury/minimal risk to personal safety** | **No injury/low risk to personal safety of client/employee** | **injuries/moderate risk to safety of client/employee** | **Death/disabling injury/high risk to safety of client/employee** | **Multiple deaths or disabling injuries/very high risk to safety of client/employee** |
| **Distress caused to any party or damage to any party's standing or reputation** | **Negligible, no public concern – only routine internal reporting** | **Minor distress, minor damage – visible limited/localised media interest, internal reporting** | **Substantial short term distress – restricted negative publicity from local media, internal inquiry** | **Substantial long term distress – main stream media report, internal inquiry** | **Substantial long term distress to multiple parties – broad public concern and media coverage,** |
| **Non-compliance – unauthorised release of information classified as protected or confidential, to a third part** | **Minor compliance issues – no or negligible impact, offence punishable by small fine** | **Short to medium term action required – minor impact, offense punishable by moderate fine** | **Immediate action needed to achieve compliance – measurable impact, offense punishable by major fine** | **Shutdown of service for non-compliance – significant impact, offence punishable by imprisonment** | **Shutdown of multiple services for noncompliance – major consequences to a person or agency** |
| **Threat to Wyndham CEC's capacity to deliver services due to Data breach** | **No or negligible threat to, or disruption of business or systems or service delivery** | **Minimal threat to, or disruption of localised business or systems or service delivery** | **Moderate threat to or cessation of a service for a week, and subsequent disruption** | **Multiple essential/critical services impaired, or disrupted over a month** | **Cessation of multiple essential/critical services for several months** |
| **Level of reporting required** | **Report required to be submitted to Privacy Officer** | **Report required to be submitted to Privacy Officer and CEO** | **Report required to be submitted to Privacy Officer, CEO and Australian Information Commissioner** | **Report required to be submitted to Privacy Officer, CEO and Australian Information Commissioner** | **Report required to be submitted to Privacy Officer, CEO and Australian Information Commissioner** |

| DATA BREACH IMPACT SEVERITY RATINGS FORM (Continued) | | | | | |
|---|---|---|---|---|---|
| **Impact Type** | **Lowest** ← | | **Severity** | → | **Highest** |
| **Impact Severity** | **1. NEGLIGIBLE** | **2. LOW** | **3. MEDIUM** | **4. HIGH** | **5. VERY HIGH** |
| **Impact on Wyndham CEC finances, economic or commercial interests** | **No or negligible impact – consequences resolved by routine operations** | **Minor impact on finances, economic or commercial interests** | **Moderate impact – disadvantage caused to Wyndham CEC** | **Substantial – damage to finances, economic or commercial interests** | **Substantial – damage to finances, economic or commercial interests** |
| **Impact on development or operation of Wyndham CEC** | **No or negligible impact – consequences resolved by routine operations** | **Minor – impact on efficiency or effectiveness, managed internally** | **Impede effective development or operation – significant review or changes required** | **Seriously impede development or operation – project or program may not survive** | **Substantially impede operation or development** |
| **Level of reporting required** | **Report required to be submitted to Privacy Officer** | **Report required to be submitted to Privacy Officer and CEO** | **Report required to be submitted to Privacy Officer, CEO and Australian Information Commissioner** | **Report required to be submitted to Privacy Officer, CEO and Australian Information Commissioner** | **Report required to be submitted to Privacy Officer, CEO and Australian Information Commissioner** |