KINGSWAY
CHRISTIAN COLLEGE

Cricos Provider #01855M

COLLEGE POLICY AND PROCEDURE

DATA BREACH POLICY

VERSION
1.0

Document and Version Management

Version Number	Approval Date	Approved by	Amendment Details	Review Date
1.0	February 2018	Principal	Created	February 2021

DATA BREACH POLICY

Policy

The College will act in the best interest of individuals when an eligible data breach occurred that is likely to result in serious harm, in accordance with the Notifiable Data Breaches Scheme.

Introduction

The Notifiable Data Breaches (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.

Collectively the College's policies, procedures, systems and security safeguards aim to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification and disclosure.

However, a data breach can occur any time as result of an intentional or unintentional release of personal information to an untrusted environment. Data breaches are not limited to hacking or cyber attacks, but also due to human error or failure to follow policies that result in personal information being inadvertently lost, accessed, changed or disclosed to the wrong person.

This Policy aims to ensure that suspected or eligible data breaches are dealt with in accordance with the Privacy Act 1988 and the Notifiable Data Breaches (NDB) Scheme.

Rationale

Privacy Act 1988 Part IIIC – Notification of eligible data breaches, enacted by the Privacy Amendment (Notifiable Data Breaches) Act 2017
Australian Privacy Principle 1 – Open and transparent management of personal information
Australian Privacy Principle 11 – Security of personal information
Failure to comply with the notification requirements under the NDB Scheme may result in penalties under the Privacy Act including fines of $420,000 for individuals and $2.1 million for organisations.

Definitions

Data Breach: A data breach occurs where 'personal information held by an organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.'

Eligible Data Breach: An eligible data breach occurs when three criteria are met:

- 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
- The entity has not been able to prevent the likely risk of serious harm with remedial action.

Notifiable Data Breach (NDB): A notifiable data breach is defined as a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

Personal Information: Personal information is defined as, information or an opinion, whether true or not, and whether recorded in material form or not, about an identified individual, or an individual whose identity is reasonably apparent, or can be determined, from the relevant information or opinion and includes such information as a person's name, address, financial information, marital status or billing details. Personal Information includes 'Sensitive Information' and 'Health Information'.

Individual: Includes students, parents/guardians, prospective parents/guardians, staff, prospective staff, volunteers, alumni, suppliers, visitors, contractors and board members.

Serious Harm: Serious harm to an individual may include serious physical, psychological, emotional, economic and financial harm, serious harm to reputation and other forms of serious harm that a reasonable person in the College's position would identify as a possible outcome of the data breach.

Notification

An eligible data breach (NDB), which would require notification, occurs in circumstances where:

- there is an unauthorised access or unauthorised disclosure of information and a reasonable person would conclude that access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates, or
- information is lost in circumstances where such unauthorised access or disclosure is likely to occur and a reasonable person would conclude that, assuming such access or disclosure did occur, it would be likely to result in serious harm to any individuals to whom that information relates.

The notification must include recommendations about the steps individuals should take in response to the breach. The Office of the Australian Information Commissioner (OAIC) must also be notified of eligible data breaches.

Not all data breaches will be NDB's. For example, if an organisation acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the OAIC.

Examples of circumstances which may meet the criteria of a NDB, include when:

- a device containing a member(s) of the school community's personal information is lost or stolen (e.g. a College device)
- a database containing personal information is hacked
- personal information about students or staff is mistakenly provided to the wrong person
- records containing student information is stolen from unsecured recycling bins, or
- disclosing personal information about students/staff for purposes other than what it was collected for and without the consent of the affected students/staff.

Click here for further information about Identifying eligible data breaches

Click here for further information about Exceptions to notification obligations

Serious Harm

Harm is not defined in the legislation, so it can be any form of measurable harm. Two important qualifiers must be present – the breach presents a serious form of harm and the harm is likely to occur.

Understanding whether serious harm is likely or not requires an evaluation of the context of the data breach.

The risk of serious harm is assessed holistically, having regard to the likelihood of the harm eventuating for the individual whose personal information was part of the data breach and the consequences of the harm.

To conclude that there is serious harm and whether it is likely to occur, requires the College to assess all the information available and the context of the data breach. Consider, and perform a contextual analysis based on

1. the type or types of personal information involved in the breach
2. the particular circumstances of the data breach
3. the nature of the harm that may result from the data breach.

The decision should be reasonable, informed, logical, evidence based and well documented.

Examples of the kinds of information that may increase the risk of serious harm if there is a data breach include:

- Sensitive information, such as information about an individual's health
- Documents commonly used for identity fraud, including medicare card, drivers licence, TFN, passport details
- Financial information.

Examples of the nature of the harm include:

- Identity theft
- Significant financial loss by the individual
- Threats to an individual's physical safety
- Loss of employment opportunities
- Humiliation, damage to reputation or relationships
- Workplace or social bullying or marginalisation.

Where it is uncertain if a data breach is likely to result in serious harm, there is the obligation to conduct an assessment of the breach.

Remedial Action

Where an unauthorised access, disclosure or loss of personal information occurs but appropriate remedial action is taken by the College, this may avoid triggering the data breach notification procedures.

Remedial Action is the positive steps taken to address data breach in a timely manner, avoiding the need to notify the data breach. This results in the harm being unlikely or non-serious.

If the College acts before the unauthorised access, disclosure or loss causes serious harm to any of the individuals to whom the information relates, and as a result of that action, a reasonable person would conclude that the access, disclosure or loss would not be likely to result in serious harm to any of those individuals, the access, disclosure or loss will not be an eligible data breach.For breaches where personal information is lost, the remedial action is adequate if it prevents the unauthorised access or disclosure of personal information.

Click here for further information about Identifying eligible data breaches

Data Breach Response

Generally, the actions taken following a data breach should follow four key steps:

Step 1: Contain the data breach to prevent any further compromise of personal information.

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 any risk of harm.

Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

At any time, entities should take remedial action, where possible, to limit the impact of the breach on affected individuals. If remedial action is successful in preventing a likely risk of serious harm to individuals, the NDB scheme notification obligations may not apply.

In general, entities should:

- take each data breach or suspected data breach seriously and move immediately to contain, assess and remediate the incident. Breaches that may initially seem immaterial may be significant when their full implications are assessed
- undertake steps 1 (Contain), 2 (Assess), and 3 (Notify) either simultaneously or in quick succession. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs
- determine how to respond on a case-by-case basis. Depending on the breach, not all steps may

be necessary, or some steps may be combined. In some cases, an entity may take additional steps that are specific to the nature of the breach.

Data Breach Response Plan

This Data Breach Response Plan outlines four key steps to undertake when responding to a breach or a suspected breach and allocates staff roles and responsibilities should a notifiable breach occur.

There is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis. In some cases, it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs.

<table>
<tr><td>Step 1</td><td>Contain the Breach
Each breach will be taken seriously and immediate action will be taken to contain and assess the suspected breach.

The Principal will take whatever steps possible to immediately contain the breach.

The Principal will be supported by other senior staff, depending on the type and nature of breach.

The Principal will notify the Board Chair of the breach or suspected breach.

Refer to the Remedial Action section above to avoid triggering the data breach notification procedures outlined in steps 2 and 3 below.</td></tr>
<tr><td>Step 2</td><td>Perform the Assessment
Breaches that may initially seem immaterial may be significant when their full implications are assessed.

When an eligible data breach is suspected or believed to have occurred the College must undertake a reasonable and expeditious assessment within 30 days to determine if the data breach is likely to result in serious harm to any individual affected.

The Principal will lead the assessment.

Depending on the type and nature of the breach, the Principal and other Senior Leadership Team members will determine whether there is a need to assemble a team to support and undertake the assessment.

The assessment should cover off the following three stages:
<table>
<tr><td>2.1</td><td>Initiate: decide whether an assessment is necessary and identify which person or group will be responsible for completing it.</td></tr>
<tr><td>2.2</td><td>Investigate: quickly gather relevant information about the suspected breach, including, for example, what personal information is affected, who may have had access to the information and the likely impacts, and</td></tr>
<tr><td>2.3</td><td>Evaluate: make a decision, based on the investigation, about whether the identified breach is an eligible data breach. Refer to the Serious Harm section above when evaluating the risks associated with the breach.</td></tr>
</table>
The Principal will document the assessment as evidence of remedial action taken.

Read the Assessing a suspected data breach here</td></tr>
<tr><td>Step 3</td><td>Notification
Where the Principal has formed the view that an eligible data breach has occurred, the College is obliged to promptly notify individuals at likely risk of serious harm.

The Principal will inform the Board Chair of the outcome of the assessment and the obligation to notify.

The Principal must also notify the OAIC as soon as practicable through a statement about the eligible data breach.</td></tr>
</table>

	The notification to affected individuals and the OAIC must be in the form of a statement and must include the following information: • The identity and contact details of the organisation • A description of the eligible data breach • The kinds of information concerned and; • Recommendations about the steps individuals should take in response to the data breach. The content of the statement to the OAIC must be communicated to the affected individuals. Click here for further information about Notifying individuals about an eligible data breach Click here for further information about What to include in an eligible data breach statement Click here for further information about Online Notifiable data breach statement – form Click here for further information about Notifying affected individuals There are three options for notification: • Notify all individuals whose personal information is involved in the eligible data breach, • Notify only the individuals who are at likely risk of serious harm, or • Publish your notification, and publicise it with the aim of bringing it to the attention of all individuals at likely risk of serious harm. This option is only available if the first two options weren't practicable. There is flexibility in the way individuals are notified – by telephone, email, text message, social media, post or in person conversation.
Step 4	**Prevent future breaches** The Principal will evaluate whether it was a systemic breach or an isolated event. Action and review activities will be proportionate to the significance of the breach and may include: A review of policies and procedures and any changes to reflect the lessons learned from the investigation Staff training An audit focussing on prevention strategies.

Maintain information governance and security

Kingsway Christian College has an ongoing obligation to take reasonable steps to handle personal information in accordance with Australian Privacy Principles (APPs) This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification for disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that the College holds.

Contain

The College's first step should be to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

KCC will need to consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment process**. As part of the assessment, KCC should consider whether **remedial action** is possible. Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- Initiate: plan the assessment and assign a team or person
- Investigate: gather relevant information about the incident to determine what has occurred
- Evaluate: make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented. KCC should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, KCC should take steps to reduce any potential harm to individuals. This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur. If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — Is serious harm still likely — YES

Notify

Where serious harm is likely, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- Option 1: Notify all individuals
- Option 2: Notify only those individuals at risk of serious harm If neither of these options are practicable:
- Option 3: publish the statement on the entity's website and publicise it Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach • Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices Review

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.