Carey Baptist College

Privacy Policy

Rationale

This Privacy Policy details how we protect people's privacy and how we comply with the requirements of the Privacy Act and the 13 Australian Privacy Principles. This policy also describes:

- who we collect information from;
- the types of personal information collected and held by us;
- how this information is collected and held;
- the purposes for which your personal information is collected, held, used and disclosed;
- how you can gain access to your personal information and seek its correction;
- how you may complain or inquire about our collection, handling, use or disclosure of your personal information and how that complaint or inquiry will be handled; and
- whether we are likely to disclose your personal information to any overseas recipients.

Scope

This policy applies to all activities of Carey Baptist College on all Campuses, its students, staff and visitors.

Policy Statement

Carey Baptist College is committed to protecting the privacy of information of all our students and their families, our staff and visitors and to only use that information for the purpose it was collected or as authorised.

It is our policy to ensure our collection, storage, usage and disclosure of information is in compliance with the requirements of the Privacy Act and the 13 Australian Privacy Principles.

Appendices

Appendices relating to this policy:
Appendix 1: Privacy Policy and Procedures
Appendix 2: Privacy Collection Notice
Appendix 3: Photo Permission Statements
Appendix 4: Data Breach Response
Appendix 5: Handbook Statements

Contact

For queries relating to this policy, please contact
Policy Development Officer 08 9394 9111

Related Documents

Enrolment Policy
Enrolment Forms
Website link to Privacy Policy

References

Complispace 2018
AISWA Privacy Compliance Manual 2018

Version Management					
Version	Date Published	Changes made	Approved by	Next Review	Author of version
2	2016				
3	March 2018	Updated to new guidelines Reformatted to College Wide Format Added information related to Notifiable Data Breaches		2020	MCINAN
3	Sept 2020	Reviewed, no changes recommended		2021	MCINAN

Appendix 1: Privacy Policy and Procedures

1. **Who do we Collect Personal Information From?**
   At Carey Baptist College, we collect personal information from students, parents, prospective parents, job applicants, staff, volunteers and others including alumni, contractors, visitors and others that come into contact with the College.

   It is noted that employee records are not covered by the Australian Privacy Principles where they relate to current or former employment relations between the College and the employee.

2. **What Kinds of Personal Information Do We Collect?**
   The kinds of personal information we collect is largely dependent upon whose information we are collecting and why we are collecting it, however in general terms the College may collect:

   2.1. **Personal Information** including names, addresses and other contact details; dates of birth; next of kin details; financial information, photographic images and attendance records.
   2.2. **Sensitive Information** (particularly in relation to student and parent records) including religious beliefs, government identifiers, nationality, country of birth, languages spoken at home, professional or union memberships, family court orders and criminal records.
   2.3. **Health Information** (particularly in relation to student and parent records) including medical records, disabilities, immunisation details, individual health care plans, counselling reports, nutrition and dietary requirements.

3. **How do we collect your personal information?**
   How we collect personal information will largely be dependent upon whose information we are collecting. If it is reasonable and practical to do so, we collect personal information directly from you.

   Where possible the College has attempted to standardise the collection of personal information by using specifically designed forms (e.g. an Enrolment Form or a Health Information Disclosure Form, this may be managed by an online system such as Consent To Go (MCB Schools) or SEQTA)). However, given the nature of our operations, we often also receive personal information by email, letters, notes, over the telephone, in face to face meetings, through financial transactions and through surveillance activities such as the use of CCTV security cameras or email monitoring.

   We may also collect personal information from other people (e.g. a personal reference) or independent sources (e.g. a telephone directory), however we will only do so where it is not reasonable and practical to collect the information from you directly.

   Sometimes we may be provided with your personal information without having sought it through our normal means of collection. We refer to this as "unsolicited information". Where we collect unsolicited information we will only hold, use and/or disclose that information if we could otherwise do so had we collected it by normal means. If that unsolicited information could not have been collected by normal means then we will destroy, permanently delete or de-identify the information as appropriate.

   We may collect information based on how individuals use our website. We use "cookies" and other data collection methods to collect information on website activity such as the number of visitors, the number of pages viewed and the internet advertisements which bring visitors to our website.

This information is collected to analyse and improve our website, marketing campaigns and to record statistics on web traffic. We do not use this information to personally identify individuals.

The College does not collect personal information from their credit providers or credit reporting bodies.

4. How we use personal information

We only use personal information that is reasonably necessary for one or more of our functions or activities (the primary purpose) or for a related secondary purpose that would be reasonably expected by you, or to which you have consented.
Our primary uses of personal information include but are not limited to:

4.1. providing education, pastoral care, extra-curricular and health services;
4.2. satisfying our legal obligations including our duty of care and child protection obligations;
4.3. keeping parents informed as to College community matters through correspondence, newsletters and magazines;
4.4. marketing, promotional and fundraising activities;
4.5. supporting the activities of College associations such as an alumni association;
4.6. supporting community based causes and activities, charities and other causes in connection with College functions or activities;
4.7. helping us to improve our day to day operations including training our staff; systems development; developing new programs and services; undertaking planning, research and statistical analysis;
4.8. College administration including for insurance purposes;
4.9. the employment of staff;
4.10. the engagement of volunteers.

We only collect sensitive information reasonably necessary for one or more of these functions or activities, if we have the consent of the individuals to whom the sensitive information relates, or if the collection is necessary to lessen or prevent a serious threat to life, health or safety, or another permitted general situation (such as locating a missing person) or permitted health situation (such as the collection of health information to provide a health service) exists.

We will only use or disclose sensitive information for a secondary purpose if you would reasonably expect us to use or disclose the information and the secondary purpose is directly related to the primary purpose.

5. Storage and Security of Personal Information

We store personal information in a variety of formats including on databases, in hard copy files and on personal devices including laptop computers, mobile phones, cameras and other recording devices. The security of your personal information is of importance to us and we take reasonable steps to protect the personal information we hold about you from misuse, loss, unauthorised access, modification or disclosure.
These steps include:

5.1. Restricting access to information on College databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile.
5.2. Ensuring all staff are aware that they are not to reveal or share personal passwords.

5.3. Ensuring where sensitive and health information is stored in hard copy files that these files are stored in locked filing cabinets in lockable rooms. Access to these records is restricted to staff on a need to know basis.
5.4. Implementing physical security measures around College buildings and grounds to prevent break-ins.
5.5. Implementing ICT security systems, policies and procedures, designed to protect personal information storage on our computer networks.
5.6. Implementing human resources policies and procedures, such as email and internet usage, confidentiality and document security policies, designed to ensure that staff follow correct protocols when handling personal information. Refer to Staff Handbook, Code of Conduct and IT usage policy.
5.7. Undertaking due diligence with respect to third party service providers who may have access to personal information, including cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.

Personal information we hold that is no longer needed is destroyed in a secure manner, deleted or de-identified as appropriate.

Our website may contain links to other websites. We do not share your personal information with those websites and we are not responsible for their privacy practices. Please check their privacy policies.

6. Data Breaches

A data breach occurs when personal information is lost or subject to unauthorised access, modification, disclosure, or other misuse or interference. For schools, data breaches commonly occur due to internal human errors or a failure to follow information handling policies that result in personal information being inadvertently lost or disclosed to the wrong person.

If you become aware of a data breach or potential data breach, please notify the Privacy Officer immediately by email privacy@carey.wa.edu.au with the title "Data Breach" in the subject line.

7. Responding to Data Breaches

The College will take appropriate, prompt action if we have reasonable grounds to believe that a data breach may have, or is suspected to have occured. Depending on the type of data breach, this may include a review of our internal security procedures, taking remedial internal action, notifying affected individuals and Office of the Australian Information Commissioner (OAIC). If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to publicise the contents of this statement.

8. When we disclose personal information

We only use personal information for the purposes for which it was given to us, or for purposes which are related (or directly related in the case of sensitive information) to one or more of our functions or activities. We may disclose your personal information to government agencies, other parents, other schools, recipients of College publications, visiting teachers, counsellors and coaches, our service providers, agents, contractors, business partners and other recipients from time to time, only if one or more of the following apply:

8.1. you have consented;
8.2. you would reasonably expect us to use or disclose your personal information in this way;
8.3. we are authorised or required to do so by law;
8.4. disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety;

8.5. where another permitted general situation or permitted health situation exception applies;
8.6. disclosure is reasonably necessary for a law enforcement related activity;

9. **Personal Information of Students**

The Privacy Act does not differentiate between adults and children and does not specify an age after which individuals can make their own decisions with respect to their personal information. At Carey Baptist College, we take a common sense approach to dealing with a student's personal information and generally will refer any requests for personal information to a student's parents/carers. We will treat notices provided to parents/carers as notices provided to students and we will treat consents provided by parents/carers as consents provided by a student. We are however cognisant of the fact that children do have rights under the Privacy Act, and that in certain circumstances (especially when dealing with older students and especially when dealing with sensitive information), it will be appropriate to seek and obtain consents directly from students. We also acknowledge that there may be occasions where a student may give or withhold consent with respect to the use of their personal information independently from their parents/carers.

There may also be occasions where parents/carers are denied access to information with respect to their children, because to provide such information would have an unreasonable impact on the privacy of others, or result in a breach of the College's duty of care to the student.

10. **Disclosure of personal information to overseas recipients**

We may disclose personal information about an individual to overseas recipients in certain circumstances, such as when we are organising an overseas excursion, facilitating a student exchange, or storing information with a "cloud computing service" which stores data outside of Australia. We will however take all reasonable steps not to disclose an individual's personal information to overseas recipients unless:

10.1. We have the individual's consent (which may be implied); or
10.2. We have satisfied ourselves that the overseas recipient is compliant with the Australian Privacy Principles, or a similar privacy regime; or
10.3. We form the opinion that the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety; or
10.4. We are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

11. **How we ensure the quality of your personal information**

We take reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up to date. These steps include trying to ensure that the personal information is accurate, complete and up to date at the time of collection and when using or disclosing the personal information. On an ongoing basis we maintain and update personal information when we are advised by individuals or when we become aware through other means that their personal information has changed.

Please contact us if any of the details you have provided change. You should also contact us if you believe that the information we have about you is not accurate, complete or up to date.

12. **How to gain access to your personal information we hold**

You may request access to the personal information we hold about you, or request that we change the personal information, by contacting us.

If we do not agree to provide you with access, or to amend your personal information as requested, you will be notified accordingly. Where appropriate we will provide you with the reason/s for our decision. If the rejection relates to a request to change your personal information you may make a statement about the requested change and we will attach this to your record.

13. Privacy Complaints

If you wish to make a complaint about a breach by us of the Australian Privacy Principles, you may do so by providing your written complaint by email, letter, facsimile or by personal delivery to any one of our contact details as noted below. You may also make a complaint verbally.
We will respond to your complaint within a reasonable time (usually no longer than 30 days) and we may seek further information from you in order to provide a full and complete response.
Your complaint may also be taken to the Office of the Australian Information Commissioner.

14. How to Contact Us

You can contact us about this Policy or about your personal information by:
Emailing. privacy@carey.wa.edu.au
Calling the College 08 9394 9111 Harrisdale, 08 6166 2222 Forrestdale
Writing to our Privacy Officer at PO BOX 1409, Canning vale, WA 6970 or
by facsimile at 08 9394 9112

If practical, you can contact us anonymously (i.e. without identifying yourself) or by using a pseudonym. However, if you choose not to identify yourself, we may not be able to give you the information or provide the assistance you might otherwise receive if it is not practical to do so.

15. **Changes to our privacy and information handling practices**

This Privacy Policy is subject to change at any time. Please check our Privacy Policy on our website (www.carey.wa.edu.au) regularly for any changes.

Appendix 2: Privacy Collection Notice

Information Collection Notice

This Collection Notice explains in general terms how we protect the privacy of the personal information you provide when you are enrolling your child or your child is enrolled at the College. In reviewing this Collection Notice and providing us with your personal information, you consent to our collection, use and disclosure of that information in the manner set out below, unless you tell us otherwise.

1. Carey Baptist College (the College) collects personal information, including sensitive information about students and parents or guardians and family members before and during the course of a student's enrolment at the College. This may be in writing or in the course of conversations. The primary purpose of collecting this information is to enable the College to meet its educational, administrative and duty of care responsibilities to the student to enable them to take part in all the activities of the College.
2. Some of the information the College collects is to satisfy the College's legal obligations, particularly to enable the College to discharge its duty of care.
3. Laws governing or relating to the operation of a College require certain information to be collected and disclosed. These include relevant Education Acts and Public Health and Child Protection laws.
4. The College may request medical reports and health information about students from time to time to discharge its legal duty of care to the student and to other students and staff. This includes a student's asthma and anaphylaxis action plans, as well as any other health or medical information which is reasonably likely to impact on the College's ability to provide educational, first aid and related services.
5. A student's health and medical information will be disseminated and used within the College to best meet the College's duty of care responsibilities. This may include the use of photographs with health action plans to facilitate the identification of students who may be at heightened risk.
   Health information about students is sensitive information within the terms of the Australian Privacy Principles (APPs) under the Privacy Act 1988.
6. The College may disclose personal and sensitive information for administrative, educational and support purposes (or may permit the information to be directly collected by third parties). This may include to:
   - government departments;
   - third party service providers that provide online educational and assessment support services or applications (apps), which may include email and instant messaging;
   - another school to facilitate the transfer of a student;
   - medical practitioners, and people providing educational support and health services to the College, including specialist visiting teachers, sports coaches, volunteers, counsellors and providers of learning and assessment tools;
   - assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority;
   - people providing administrative and financial services to the College;
   - anyone you authorise the College to disclose information to; and
   - anyone to whom the College is required or authorised to disclose the information to by law, including under child protection laws.
7. If this information is not provided to us, the College views this as an unacceptable risk and will not proceed with the enrolment.
8. The College will engage in fundraising activities from time to time. Information received from you may be used for these purposes. It may also be disclosed to a future College Alumni who may assist in the fundraising activities of the College. We will not disclose your personal information to third parties for their own marketing purposes without your consent.

9. The College may also use cloud computing service providers to store personal information (which may include sensitive information) on their servers in the 'cloud'. These servers may be located in or outside Australia. This may mean that personal information may be stored or processed outside Australia. The College's Privacy Policy contains further information about its use of cloud and other third-party service providers and any of their overseas locations.
10. The College's Privacy Policy is accessible via the College website or from the College administration office. The policy sets out how parents, guardians or students may seek access to, and correction of their personal information which the College has collected and holds. However, access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others, or may result in a breach of the College's duty of care to the student, or where students have provided information in confidence. Any refusal will be notified in writing with reasons if appropriate.
11. The College's Privacy Policy also sets out how parents, guardians, students and their family can make a complaint about a breach of the APPs and how the complaint will be handled.
12. On occasions information such as academic and sporting achievements, student activities and similar news is published in College newsletters and magazines, on physical displays throughout the College and on our intranet. This may include photographs and videos of student activities such as sporting events, College camps and College excursions.
    The College will obtain separate permissions from the student's parent or guardian (and from the student if appropriate) prior to including such photographs or videos or other identifying material in our promotional material or otherwise making this material available to the public, such as on the internet.
    The College will obtain separate permissions from the student's parent or guardian prior to including personal information on College directories (eg Class Representative or Parents in Partnership lists)
13. If you provide the College with the personal information of others, such as other family members, doctors or emergency contacts, we encourage you to inform them that you are disclosing that information to the College and why, that they can request access to and correction of that information if they wish and to also refer them to the College's Privacy Policy for further details about such requests and how the College otherwise handles personal information it collects and complaints it receives.

How to Contact Us

You can contact us about this Policy or about your personal information by:
Emailing. privacy@carey.wa.edu.au
Calling the College 08 9394 9111 Harrisdale, 08 6166 2222 Forrestdale
Writing to our Privacy Officer at PO BOX 1409, Canning vale, WA 6970 or
by facsimile at 08 9394 9112

Note: this notice must appear at information collection points such as enrolment forms and our online data collection system.

Appendix 3: Photo Permission Statement

Note: this notice will be included in the enrolment form.

I/We understand that on occasion photographs of students, examples of work done by students, and notices of academic, sporting or other College-related achievements may be included in College publications including (but not limited to) in newsletters and on College website and social media platforms. Student images will always reflect College values and in most cases students will be part of a group with limited identifying information attached. In situations where an image of a student is to be used for high profile promotional purposes or for use by third parties, specific permission will be sought.

I//We consent to the use of my child's photography, work and name for College display or marketing purposes.

▢ Yes ▢ No

_____ _____

Signature Date Signature Date

For Consent 2 Go

I/We understand that on occasion photographs of students, examples of work and notices of achievements may be included in College publications (eg newsletters, website and social media platforms). Please refer to our privacy policy for further information.

I give permission for Carey Baptist College to print my child's first name and surname and to use images, work and name for College display or marketing purposes.

Appendix 4: Data Breach Response

Data Breach Response Team

In the event of a Data Breach, the Privacy Officer will establish a Data Breach Response Team (DBRT). The DBRT is responsible for assisting the Privacy Officer in investigating the breach and notifying the OAIC when required.

The DBRT members will include representatives from the Executive Team , the College's technology team and other departments as needed.

Depending on the nature of the breach, the composition of the DBRT may vary. For example, the College is alerted to the incident through a complaint, the Complaints Manager would form part of the Team.

Data Breach Response Plan

If a data breach is identified using the Guide to Data Breach Identification the Data Breach Response Plan must be followed.

The Data Breach Response Plan sets out procedures and clean lines of authority for the College in the event that it experiences circumstances that amount to a data breach or a Notifiable Data Breach.

The response in the Data Breach Response Plan is intended to enable the College to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals and to meet our notification obligations under the Privacy Act.

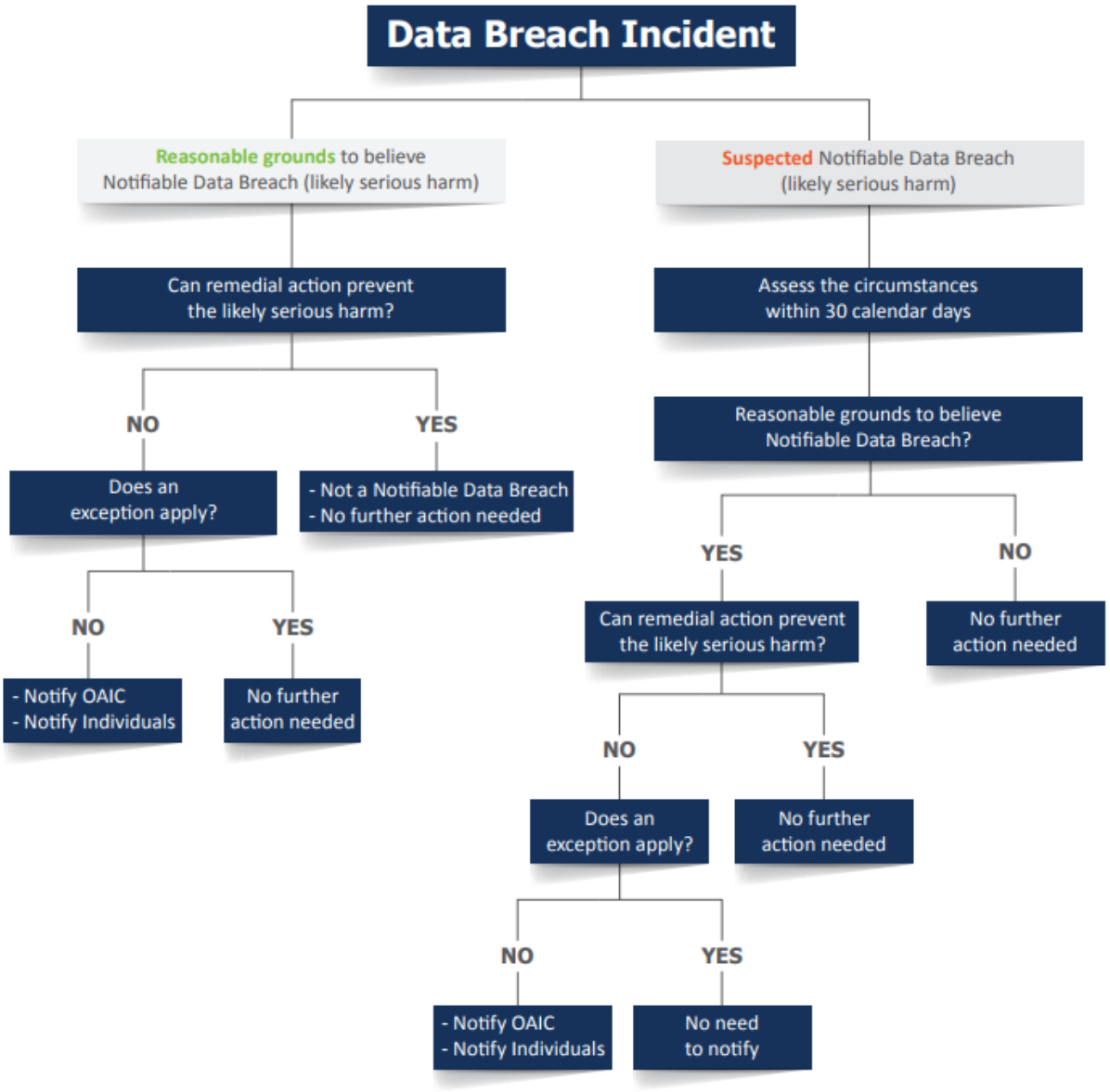
Information Collecting

Various steps in the Data Breach Response Plan require the collection of information.

In the event that the Data Breach Response Plan is activated, the Privacy Officer will ensure that:

- evidence is preserved that may be valuable to determine the context of the data breach and a list of affected individuals, or possible affected individuals
- information will be compiled for external notification processes and internal reporting
- records of the information are kept.

Guide to Data Breach Identification



Notifiable Data Breach Response Plan

A data breach can take many forms and have many causes. Depending on the circumstances, the extent of interference with personal information will vary, as will the harm suffered by the individuals affected by the interference. Our notification obligations can also vary.

Suspected or known data breach

A data breach occurs when personal information held by the School is misused, interfered with, lost or subject to unauthorised access, modification or disclosure.

1. Contain

The first step is 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.

2. Assess

The School needs to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If there are reasonable grounds to believe this is the case, then the School 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, the School should consider whether **remedial action** is possible. The School will conduct an assessment in three stages:

1. **Initiate:** plan the assessment and form a DBRT
2. **Investigate:** gather relevant information about the incident to determine what has occurred
3. **Evaluate:** make an evidence-based decision about whether serious harm is likely. This decision should be documented.

The School must conduct this assessment within 30 days.

Take remedial action

Where possible, the School 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 databases.

If remedial action is successful in making serious harm no longer likely, then notification is not required. Progress to Step 4: Review.

NO — **Is serious harm still likely?** — **YES**

3. Notify

Where **serious harm is likely**, the School must prepare a statement for the OAIC to be submitted as soon as practicable that contains:

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

The School must also notify affected individuals, and inform them of the contents of this statement.

The School has three options for notifying:

1. Notify all individuals
2. Notify all individuals at risk of serious harm.

OR if 1 or 2 aren't practicable:

3. Publish the statement on the School's public website and publicise it.

The School may provide further information in its notification, such as an apology and an explanation of what they are doing about the breach.

4. 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 plans
- considering changes to School policies and procedures
- revising staff training practices
- consider a report to the School Board on outcomes and recommendations following the review

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

- police or law enforcement
- ASIC
- professional bodies
- other entity/ies that may be involved in the breach

Remedial Action

What is Remedial Action?

Remedial action is action taken to contain a suspected data breach and to prevent the likely risk of serious harm occurring.

For example, if a staff member accidentally sends an email containing personal information to the wrong recipient, the Privacy Officer and the staff member may be able to take action to remedy the breach so that a reasonable person would conclude that the breach would likely not result in serious harm to any person to whom the information relates. Action could include recalling the email or contacting the recipient who agrees to delete the email.

Successful Remedial Action

If remedial action is successful, and the likely risk of serious harm occurring has been prevented, the breach will not amount to a Notifiable Data Breach and notification to the OAIC and affected individuals will not be required.

Unsuccessful Remedial Action

If remedial action is unsuccessful, meaning that the likely risk of serious harm occurring has not been prevented, the data breach will be a Notifiable Data Breach and, it may be appropriate for the Privacy Officer to escalate the matter to the Data Breach Response Team.

Voluntary Notification to OAIC and/or Individuals

Not all data breaches require notification to the OAIC and affected individuals. If there are reasonable grounds to suspect that there may have been a Notifiable Data Breach, we must comply with the notification requirements set out in the Privacy Act.

If a data breach is not a Notifiable Data Breach, the College is not legally required to notify the OAIC and affected individuals but may choose to do so as a matter of best practice. A decision to voluntarily notify the OAIC and/or affected individuals will be made on a case-by-case basis having regard to the following factors:

- notification as a reasonable security safeguard: to help protect information from misuse, interference or loss
- notification as openness about privacy practices: being open and transparent when something goes wrong
- notification as restoring control over personal information: where it will assist individuals to regain control of the information
- notification as a means of rebuilding public trust: where it will demonstrate to the public that the College takes its privacy obligations seriously

OAIC Contact Details:

If we decide to notify the OAIC we will do so using one of the following contact options:

- **Email: enquiries@oaic.gov.au**
- **Telephone: 1300 363 992**
- **Facsimile: + 61 2 9284 9666**
- **Post: GPO Box 5218, Sydney NSW 2001**

Terminology

Data Breach

It is important to note that although the Privacy Act regulates the handling of personal information, not "data", the OAIC uses the term data breach rather than "personal information security breach" in its guidance to organisations on how to respond to an incident.

A data breach occurs when personal information held by Carey Baptist College is misused, interfered with, lost or subject to unauthorised access, modification or disclosure. In other words, a data breach may occur as a result of a failure by Carey Baptist College to protect the security of:

- personal information, in accordance with APP 11: Security of Personal Information; and/or
- credit information, in accordance with the Privacy Act and Credit Reporting Code (refer to Credit Reporting Policy).

Examples of data breaches include:

- lost or stolen laptops, removable storage devices, or paper records containing personal information
- databases containing personal information being 'hacked' or otherwise illegally accessed by individuals outside of the College
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment
- paper records stolen from insecure recycling or garbage bins
- the College mistakenly providing personal information to the wrong person, for example by sending details to the wrong address.

Data breaches that are likely to result in serious harm to any of the individuals to whom the information relates may be a Notifiable Data Breach.

Likely means 'more probable than not'.

Notifiable Data Breach
A Notifiable Data Breach occurs where the College holds personal information relating to one or more individuals, is required to comply with APP 11 in relation to that information, and:

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

Under the Privacy Act, these types of data breaches are referred to as "eligible data breaches", however for the purposes of this policy, the College has adopted the phrase Notifiable Data Breach as in the OAIC's guidance materials.

Serious Harm

This term is not defined in the Privacy Act. The term could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.
The Act sets out a list of factors to consider when determining whether a reasonable person would conclude that an incident of access to, or a disclosure of, information:

- would be likely; or
- would not be likely,

to result in serious harm to any of the individuals to whom the information relates.

Those factors are:

- the kind/s of information
- the sensitivity of the information
- whether the information is protected by one or more security measures
- if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security technology or methodology was used in relation to the information and was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information, the likelihood that the persons, or the kinds of persons, who:
    - have obtained or, or who could obtain the information
    - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates
    - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
    - the nature of the harm
    - any other relevant matters.

Appendix 5: Statement for Inductions/Handbook/Code of Conduct

Staff:

Carey Baptist College is committed to protecting the privacy of information of all our students and their families, our staff and visitors and to only use that information for the purpose it was collected or as authorised.

It is our policy to ensure our collection, storage, usage and disclosure of information is in compliance with the requirements of the Privacy Act and the 13 Australian Privacy Principles. Our privacy policy and procedures can be located on the Carey College website.

Staff, students, families and visitors(where relevant) are expected to follow the privacy policy and be aware of the security of their devices and personal information relating to themselves and other members of the Carey community. They are expected to uphold confidentiality where appropriate, and not discuss or disclose information relating to other parties without consent outside of the bounds of the privacy policy.

The Notifiable Data Breach (NDB) Scheme requires the College to notify the Office of the Australian Information Commissioner if the College or individuals within the College are responsible for a data breach.

A data breach occurs when personal information is lost or subject to unauthorised access, modification, disclosure, or other misuse or interference. For schools, data breaches commonly occur due to internal human errors or a failure to follow information handling policies that result in personal information being inadvertently lost or disclosed to the wrong person.

A data breach is deemed to have occurred 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.

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

- a device containing a member of the College community's personal information is lost or stolen (e.g a college laptop, or personal mobile with access to College systems)
- 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.

If you become aware of a data breach or potential data breach, please notify the Privacy Officer immediately by email privacy@carey.wa.edu.au with the title "Data Breach" in the subject line. If appropriate, also notify the relevant College Principal.

Families:
Carey Baptist College is committed to protecting the privacy of information of all our students and their families, our staff and visitors and to only use that information for the purpose it was collected or as authorised.

It is our policy to ensure our collection, storage, usage and disclosure of information is in compliance with the requirements of the Privacy Act and the 13 Australian Privacy Principles. Our privacy policy and procedures can be located on the Carey College website.

Staff, students, families and visitors(where relevant) are expected to follow the privacy policy and be aware of the security of their devices and personal information relating to themselves and other members of the Carey community. They are expected to uphold confidentiality where appropriate, and not discuss or disclose information relating to other parties without consent outside of the bounds of the privacy policy.

The Notifiable Data Breach (NDB) Scheme requires the College to notify the Office of the Australian Information Commissioner if the College or individuals within the College are responsible for a data breach.

A data breach occurs when personal information is lost or subject to unauthorised access, modification, disclosure, or other misuse or interference. For schools, data breaches commonly occur due to internal human errors or a failure to follow information handling policies that result in personal information being inadvertently lost or disclosed to the wrong person.

If you become aware of a data breach or potential data breach, please notify the Privacy Officer immediately by email privacy@carey.wa.edu.au with the title "Data Breach" in the subject line.