



# CARMICHAEL COLLEGE DATA BREACH POLICY

<b>Title</b>	Carmichael College Data Breach Policy
<b>Category</b>	College Operational
<b>Policy Owner</b>	Executive Committee
<b>Approver</b>	Board of Directors
<b>Related Documents</b>	<ul style="list-style-type: none"> <li>● <i>Privacy Act 1988 (Cth)</i></li> <li>● <i>Privacy Amendment (Enhancing Privacy Protection) Act 2012</i></li> <li>● Carmichael College Child Protection Policy</li> <li>● Carmichael College Disability Discrimination Policy</li> <li>● Carmichael College Complaints Handling Policy - Parents &amp; Students</li> <li>● Carmichael College IT Policy and Procedures</li> <li>● Carmichael College Privacy Policy</li> </ul>
<b>Published Location</b>	<p><b><i>Internal</i></b> - <a href="#">SharePoint - Data Breach Policy</a></p> <p><b><i>External</i></b> - Carmichael College Website</p>

**CARMICHAEL COLLEGE LTD**

793 Oakey Flat Rd., Morayfield Qld 4506 // ABN: 31 1155 658 50

<b>Revision Record</b>					
<b>Version</b>	<b>Approval Date</b>	<b>Approved By</b>	<b>Effective Date</b>	<b>Review Cycle</b>	<b>Next Review</b>
February 2023	February 2023	Board of Directors	February 2023	Annual	February 2024
March 2026	March 2026	Board of Directors	March 2026	Annual	March 2027

## 1. Purpose and Scope

The purpose of this policy is to ensure that identified data breaches are dealt with in a responsive, effective and appropriate way.

This policy outlines the processes required to deal with data breaches and to ensure that the possibility of data breaches is reduced as much as possible.

The policy applies to board members, employees, volunteers, parents/guardians and students, contractors, and people visiting the school site; and describes the processes through which data breaches are reported and the steps taken to protect college systems and information from possible data breaches.

## 2. Policy

The College maintains the privacy of personal information about staff, students and family members through the following means:

- Containing personal information in an access-controlled Student Information System (SENTRAL).
- Protecting data in the Student Information System and its database through appropriate backups.
- Controlling and discouraging users from copying or sharing information from the Student Information System.
- Encouraging and where appropriate, enforcing responsible security and password behaviours among staff with access to personal information.
- Physically securing computers to prevent direct unauthorised access.

## 3. Definitions

The College is obliged to act when there has been an 'eligible data breach' involving:

- unauthorised access, disclosure or loss of personal information
- that may result in serious harm to an individual as judged by a reasonable person and
- the College has not been able to prevent the potential harm through remedial action.

**'Personal information'** is information about an identified individual, or an individual who is reasonably identifiable. For example, information pertaining to their identity (driver's license, Medicare number, passport details), personal status (age, living situation, health, religion, gender etc.) or legal status (financial, marital, relational, parental etc.).

**'Unauthorised access'** involves revealing personal information by a staff member, contractor, student or other third party who would not normally be permitted access.

**'Unauthorised disclosure'** involves making personal information available beyond the College.

**'Loss'** refers to information being accidentally made available beyond the control of the College.

**'Serious harm'** to an individual may include serious physical, psychological, emotional, financial or reputational harm. The seriousness of the harm is gauged by the number of individuals whose personal information is involved, what information may have been accessed and its sensitivity, by whom and their potential intentions.

A **'reasonable person'** is a College staff member who is properly informed and able to assess the data breach.

**'Remedial action'** is that taken by the College to remove or reduce access to the information, such as ensuring information shared accidentally is deleted.

### EXAMPLES

- A student obtains a staff member's password leading to unauthorised access.

- A staff member leaves their computer unlocked while they are away, leading to unauthorised access.
- A staff member inadvertently provides their credentials to a malicious third party through an email phishing scheme, leading to unauthorised access.
- Personal information is captured in a document that is shared by email or using cloud storage resulting in unauthorised disclosure.
- A teacher misplaces printed personal information used for reference during an excursion, resulting in information loss.

#### **4. Procedure for responding to a data breach.**

##### **Contain**

As soon as College staff suspect a data breach, even before it is determined whether it is an eligible data breach, the following actions should be taken to contain the breach:

- Notify Education Technology Support staff immediately.
- Notify the Principal and relevant Head of Primary or Head of Secondary College or Executive Director immediately given the potential serious consequences of the involvement of students and staff.
- Change the network password of individuals whose information may have been lost, without their consent or involvement if necessary.
- Change the system access passwords of any systems that may have been compromised.
- Lock the account of any staff member or student suspected of unauthorised access.
- Capture logs of recent activity of involved staff and students for potential assessment.

##### **Assess**

If College staff suspect there has been any data breach, they must quickly (within 30 days, but as soon as possible) assess the following:

- What personal information may have been accessed.
- How many individuals were affected.
- Who has gained access to the information and their potential.
- How long the information has been available.
- The seriousness of the potential harm to individuals and ultimately
- Whether the breach is an eligible data breach requiring further action

At any time, the College may attempt remedial action if it could reduce the seriousness of harm.

##### **Notify**

When a breach is determined to be an eligible data breach, a response should be planned by the following people:

- The Systems Officer to describe the scale and seriousness of harm.
- The Principal, Head of Primary or Head of Secondary to determine disciplinary action and parental involvement where students are involved.
- The Executive Director, Principal, and Head of Primary or Head of Secondary where staff members are suspected to have been involved in unauthorised access.
- The Business Manager and Finance Manager where there is potential financial loss to the College because of the breach.
- Police where there is potential physical or criminal risk.
- Notification needs to be sent to all affected individuals. Should there be widespread data loss affecting people who cannot be specifically identified, the notification may need to be sent to all individuals or made publicly.

A report of any eligible data breach must be sent to the Australian Information Commissioner through the Notifiable Data Breach statement Form. The notification to affected individuals and the Commissioner must include the following information:

- The identity and contact details of the College.
- A description of the data breach.
- The kinds of information concerned.
- Recommended steps individuals should take in response to the data breach.

### Review

Following notification, the following actions may be taken:

- Enact plans to prevent similar future data breaches.
- Conduct audits to ensure preventative measures are working.
- Consider changes to staff and student policies.
- Revise staff training.
- Update this Data Breach Policy.

### Appendix 1 - Summary of Key Changes

Version	Key Changes
February 2023	New Policy.
March 2026	Update position titles and internal published location.