



Bundaberg Christian College  
Education with Wisdom

# BCC Privacy Policy

“EDUCATION WITH WISDOM”

“**Wisdom** is supreme; therefore, get wisdom. Though it cost all you have, get **understanding.**”  
(Proverbs 4:7)

Version 2.0  
Updated Last: 04/04/2018  
Review Date: Annually

Respect | Integrity | Servanthood | Excellence

P (07) 4132 5800 F (07) 4159 3618  
E [info@bcc.net.au](mailto:info@bcc.net.au) W [www.bcc.net.au](http://www.bcc.net.au)  
234 Ashfield Road Bundaberg QLD 4670  
CRICOS: 03242B ABN: 36 066 982 974

## Contents

<b>PURPOSE</b>	<b>3</b>
<b>SCOPE</b>	<b>3</b>
<b>LEGISLATION and REFERENCES</b>	<b>3</b>
<b>POLICY</b>	<b>3</b>
<b>Types of Information Collected</b>	<b>3</b>
Personal Information you provide:	3
Personal Information provided by other people:	3
<b>Students and Parents</b>	<b>4</b>
<b>Job applicants, staff members and contractors</b>	<b>4</b>
<b>Volunteers</b>	<b>4</b>
<b>Marketing and fundraising</b>	<b>4</b>
<b>Photography, Video &amp; Audio Recordings</b>	<b>5</b>
<b>Disclosure of Personal Information</b>	<b>5</b>
<b>Sending Information Overseas</b>	<b>5</b>
<b>Management and Security of Personal Information</b>	<b>5</b>
Privacy Officer	5
<b>Unauthorised access to personal information</b>	<b>6</b>
<b>Access and Correction of Personal Information</b>	<b>6</b>
<b>Consent and Rights of Access to the Personal Information of Students</b>	<b>6</b>
<b>Enquiries and Complaints</b>	<b>6</b>
<b>APPENDIX 1</b>	<b>7</b>
<b>Mandatory Notification of Eligible Data Breaches Summary</b>	<b>7</b>
<b>APPENDIX 2 – Data Breach Response Plan</b>	<b>8</b>
Step 1 - Confirm, contain and keep records of the Data Breach and do a preliminary assessment	8
Step 2 - Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely	8
Step 3 - Consider Data Breach notifications	9
Step 4 -Take action to prevent future Data Breaches	9
Response Team	10
<b>APPENDIX 3 – Notification Statement of an Eligible Data Breach</b>	<b>11</b>
<b>APPENDIX 4</b>	<b>12</b>
Standard Collection Notice	12
<b>APPENDIX 5 – Disclosure Statement to Students and Parents</b>	<b>14</b>
Counselling at Bundaberg Christian College – Things You Should Know	14
<b>APPENDIX 6</b>	<b>15</b>
Alumni Association Collection Notice	15
<b>APPENDIX 7</b>	<b>16</b>
Employment Collection Notice	16
<b>APPENDIX 8</b>	<b>17</b>
Contractor/Volunteer Collection Notice	17

## PURPOSE

This policy outlines how the College uses and manages personal or sensitive information provided to or collected by it.

The College is bound by the Australian Privacy Principles contained in Schedule 1 of the *Privacy Act 1998* (Cth).

## SCOPE

Under the *Privacy Act 1988*, the Australian Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the College's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the College and the employee.

## LEGISLATION and REFERENCES

*Privacy Act 1988 (Cth)*

*Privacy Amendment (Enhancing Privacy Protection) Act 2012*

*BCC Child Protection and Procedures Policy*

*BCC Formal Complaint Policy and Procedures*

*BCC Enrolment Application*

## POLICY

The type of information the College collects and holds includes (but is not limited to) personal information, including health details and other sensitive information, regarding:

- Student and Parents and/or Guardians before, during and after the course of a student's enrolment at the College;
- Job applicants, staff members, volunteers and contractors; and
- Other people who come into contact with the College (collectively, the "College Community").

### Types of Information Collected

The type of information the College collects and holds includes personal information about students and their parents and/or guardians (**'parents'**) (before, during and after the course of a student's enrolment at the College), job applicants, staff members, volunteers, contractors and other people who come into contact with the College. Such personal information may include, but is not limited to:

- contact details
- personal interests, hobbies, current activities, academic profile;
- employment history; and
- educational qualifications

The College may also collect sensitive information (as defined in the *Privacy Act 1988*) (such as medical information) about a student, parent/guardian, job applicant, staff member, volunteer or contractor.

### **Personal Information you provide:**

The College will generally collect personal information held about an individual by way of forms filled out by parents or students, face-to-face meetings and interviews, emails and telephone calls.

Where a child is 16 years of age or older, the College may seek to obtain the information directly from that student. All other privacy standards will apply to this information.

### **Personal Information provided by other people:**

In some circumstances the College may be provided with (or request) personal and/or sensitive information about an individual from a third party (for example a report provided by a medical professional or a reference from another school). If the College could have reasonably solicited that information from the individual using its standard information collection methods, the College will manage that information as if it had obtained that information directly from the individual and will not seek the consent of the individual.

If the College did not request the information and could not otherwise have solicited it, the College will seek the consent of the individual to continue to hold it. If the individual does not give their consent; the information will be destroyed.

### **Storage of Information**

Personal and sensitive information in the College's possession will be stored:

- Electronically in the College's internal servers;
- In hard copy on the College campus; and/or
- By a third-party data storage provider.

### **Students and Parents**

In relation to personal information of students and parents, the College's primary purpose of collection is to enable the College to provide schooling to students enrolled at the College, exercise its duty of care, and perform necessary associated administrative activities, which will enable students to take part in all the activities of the College.

The purposes for which the College uses personal information of students and parents include:

- to keep Parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration of the College;
- looking after students' educational, social and medical wellbeing;
- seeking donations and marketing for the College; and
- to satisfy the College's legal obligations and allow the College to discharge its duty of care.

In some cases, where the College requests personal information about a student or parent, if the information requested is not provided, the College may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

### **Job applicants, staff members and contractors**

The College's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor, as the case may be.

The purposes for which the College uses personal information of job applicants, staff members and contractors include:

- assessing an applicant's or potential contractor's suitability for the job
- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking donations and marketing for the College; and
- to satisfy the College's legal obligations, for example, in relation to child protection legislation.

### **Volunteers**

The College also obtains personal information about volunteers who assist the College in its functions or conduct associated activities, such as alumni associations, to enable the College and the volunteers to work together.

### **Marketing and fundraising**

The College treats marketing and seeking donations for the future growth and development of the College as an important part of ensuring that the College continues to provide a quality learning environment in which both students and staff thrive. Personal information held by the College may be disclosed to organisations that assist in the College's fundraising.

The College Community may from time to time receive fundraising information. College publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

If you would like to opt-out of direct marketing please contact the College Reception.

## Photography, Video & Audio Recordings

The College Community acknowledges that photographs, in particular, play an important role in the life of College, including for the preservation of College history. Photographs and video/audio recordings of College community members may be taken during normal College activities, annual College/class/individual photographs, for student identification cards and during curricular, co-curricular and sporting activities, and also for other promotional purposes. College Community members consent to the use and/or disclosure of photographs, video/audio by the College including for the purpose of keeping the College community informed about matters relating to the student or the College and for the purpose of promotions, marketing and fundraising. Individuals are free to discuss with the College Principal the use of their image in such material.

Camera surveillance operates at a list of fixed locations on the College grounds, to ensure public safety and for the investigation and prosecution of criminal offences. Footage will only be accessed by persons authorised to do so. Should an incident occur, footage may be provided to the Queensland Police Service for law enforcement purposes. Personal information will not be given to any other person or agency unless authorised or required by law.

## Disclosure of Personal Information

The College may disclose personal information, including sensitive information, held about an individual. This may include to:

- another school;
- government departments;
- medical practitioners;
- 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;
- recipients of College publications, such as newsletters and magazines;
- parents;
- anyone you authorise the College to disclose information to; and
- any other party as required by law.

## Sending Information Overseas

The College does not routinely send personal information about an individual outside Australia. The College may disclose personal information about an individual to overseas recipients, for instance, when facilitating a College exchange or overseas trip. The College may also use online or 'cloud' service providers to store personal information and to provide services to the College that involve the use of personal information.

The College will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual; or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

## Management and Security of Personal Information

The College has in place steps to protect the personal information the College holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records. These methods include locked storage of paper records and access rights to computerised records limited to certain individuals.

## Privacy Officer

The College has appointed a Privacy Officer, being a designated member of staff who fulfils the following roles:

- Provide a 'first point of contact' for people with enquiries related to privacy matters at the College, including reports of data breaches, suspected or real.

- Provide information about College Policies and Procedures for keeping personal information secure.
- Responsible for coordinating the Data Breach Response Plan: confirming, containing and keeping records of data breaches, conducting preliminary assessments, escalating and responding to data breaches.
- Key member of the Response Team, alerting them of any eligible data breaches.
- Undertake awareness-raising in the workplace about the College's Policies and Procedures as appropriate.

## Unauthorised access to personal information

The College does not anticipate unauthorised access to personal information will occur, and takes all reasonable steps to ensure that it does not.

If the College reasonably believes that unauthorised access to personal information has occurred amounting to an eligible data breach pursuant to the *Privacy Act 1988*, the College will conduct an investigation in accordance with **Appendix 2 – Data Breach Response Plan**.

## Access and Correction of Personal Information

An individual has a legal right to request access to any information which the College holds about them and to request correction of any perceived inaccuracy (subject to the exclusions in the National/Australian Privacy Principles).

To request access to, update or request the correction of a perceived inaccuracy please contact the Privacy Officer in writing:

**Letter addressed to:**

Privacy Officer  
Bundaberg Christian College Ltd  
234 Ashfield Road  
Ashfield QLD 4670

**Email:** [privacy@bcc.net.au](mailto:privacy@bcc.net.au)

**Phone:** 07-4132 5800

The College may require you to verify your identity and specify what information you require. The College may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the College will advise you of the likely cost in advance.

## Consent and Rights of Access to the Personal Information of Students

The College respects every Parent's right to make decisions concerning their child's education. Generally, the College will refer any requests for consent and notices in relation to the personal information of a student to the student's Parents. The College will treat consent given by Parents as consent given on behalf of the student, and notice to Parents will act as notice given to the student.

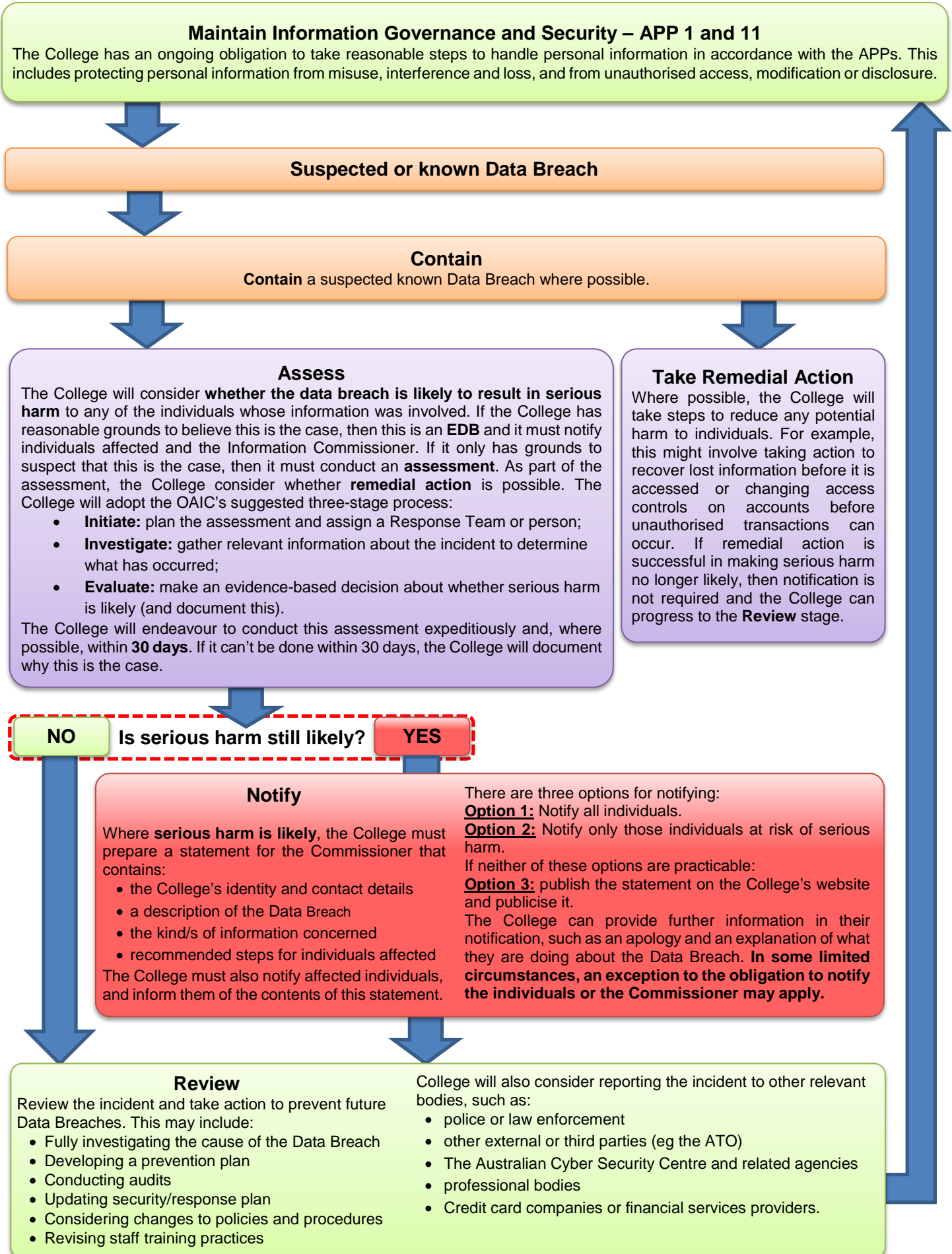
The College may, at its discretion, on the request of a student grant that student access to information held by the College about them, or allow a student to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances so warranted.

## Enquiries and Complaints

If you would like further information about the way the College manages the personal information it holds, or wish to complain that you believe that the College has breached the Australian Privacy Principles, please contact the Principal's Office in writing. The College will investigate any complaint pursuant to the BCC Formal Complaints Policy and Procedures.

APPENDIX 1

Mandatory Notification of Eligible Data Breaches Summary



## APPENDIX 2 – Data Breach Response Plan

In the event of a Data Breach, staff members must adhere to the four-step process set out below (as described in the Office of the Australian Information Commissioner's (OAIC) *Notifiable Data Breaches scheme: Resources for agencies and organisations*.) It is important that appropriate records and any evidence are kept of the Data Breach and the response. Legal advice should also be sought if necessary.

### Step 1 - Confirm, contain and keep records of the Data Breach and do a preliminary assessment

1. The staff member who becomes aware of the Data Breach or suspects a Data Breach has occurred must immediately notify the appropriate Privacy Officer. That person must take any immediately available steps to identify and contain the Data Breach and consider if there are any other steps that can be taken immediately to mitigate or remediate the harm any individual could suffer from the Data Breach.
2. In containing the Data Breach, evidence should be preserved that may be valuable in determining its cause.
3. The Privacy Officer must make a preliminary assessment of the risk level of the Data Breach. The following table sets out examples of the different risk levels.

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information (such as health information) have been leaked externally.
Medium	Loss of some personal information records and the records do not contain sensitive information. Low Risk Data Breach, but there is an indication of a systemic problem in processes or procedures.
Low	A few names and school email addresses accidentally disclosed to trusted third party (e.g. where email accidentally sent to wrong person). Near miss or potential event occurred. No identified loss, misuse or interference of personal information.

4. Where a **High Risk** incident is identified, the Privacy Officer must consider if any of the affected individuals should be notified immediately where serious harm is likely.
5. The Privacy Officer must escalate High Risk and Medium Risk Data Breaches to the Response Team (whose details are set out at the end of this plan).
6. If there could be media or stakeholder attention as a result of the Data Breach, it must be escalated to the Response Team.

### Step 2 - Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely

7. The Response Team is to take any further steps (i.e. those not identified in Step 1) available to contain the Data Breach and mitigate or remediate harm to affected individuals.
8. The Response Team is to work to evaluate the risks associated with the Data Breach, including by:
  - a. identifying the type of personal information involved in the Data Breach;
  - b. identifying the date, time, duration, and location of the Data Breach;
  - c. establishing who could have access to the personal information;
  - d. establishing the number of individuals affected; and
  - e. establishing who the affected, or possibly affected, individuals are.
9. The Response Team must then assess whether the Data Breach is likely to cause serious harm to any individual whose information is affected by the Data Breach, in which case it should be treated as an Eligible Data Breach (EDB).



10. The Response Team should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise an EDB.
11. All reasonable steps must be taken to ensure that the assessment is completed as soon as possible and in any event within **30 days** after they suspect there has been a Data Breach.

### **Step 3 - Consider Data Breach notifications**

12. The Response Team must determine whether to notify relevant stakeholders of the Data Breach, including affected individuals, parents and the OAIC even if it is not strictly an EDB.
13. As soon as the Response Team knows that an EDB has occurred or is aware that there are reasonable grounds to believe that there has been an EDB, they must prepare a statement using the **Notification Statement of an Eligible Data Breach** form and submit it to the Information Commissioner.
14. After completing the statement, unless it is not practicable, the Response Team must also take such reasonable steps to notify the contents of the statement to affected individuals or those who are at risk from the EDB.
15. If it is not practicable to notify some or all of these individuals, the Response Team must publish the statement on their website, and take reasonable steps to otherwise publicise the contents of the statement to those individuals.

### **Step 4 -Take action to prevent future Data Breaches**

16. The Response Team must complete any processes in Step 2 above that were not completed because of the delay this would have caused in proceeding to Step 3.
17. The Privacy Officer must enter details of the Data Breach and response taken into a Data Breach log. The Privacy Officer must, every year, review the Data Breach log to identify any reoccurring Data Breaches.
18. The Privacy Officer must conduct a post-breach review to assess the effectiveness of the College's response to the Data Breach and the effectiveness of the Data Breach Response Plan.
19. The Privacy Officer must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Data Breach and conduct an audit to ensure the plan is implemented.

## Response Team

Role	2 <sup>nd</sup> Contact	Responsibility and Authority
<b>Principal</b> <a href="mailto:Paul.sterling@bcc.net.au">Paul.sterling@bcc.net.au</a>	<b>Head of School</b> <a href="mailto:Darren.hutton@bcc.net.au">Darren.hutton@bcc.net.au</a> <a href="mailto:Brendan.hosking@bcc.net.au">Brendan.hosking@bcc.net.au</a>	<ul style="list-style-type: none"> <li>• Team Leader — who is responsible for leading the response team</li> <li>• Member of staff with overall accountability for privacy</li> </ul>
<b>Human Resources &amp; Marketing Manager</b> <a href="mailto:Andrew.iles@bcc.net.au">Andrew.iles@bcc.net.au</a> , <a href="mailto:privacy@bcc.net.au">privacy@bcc.net.au</a>	<b>Business Manager</b> <a href="mailto:Evan.keune@bcc.net.au">Evan.keune@bcc.net.au</a>	<ul style="list-style-type: none"> <li>• Privacy Officer</li> <li>• Coordinate the team and provide support to its members</li> <li>• Human Resources (HR) support — if the breach was due to the actions of a staff member</li> <li>• Risk Management Support — to assess the risks from the breach</li> <li>• Media/communications expertise — to assist in communicating with affected individuals and dealing with the media and external stakeholders.</li> </ul>
<b>IT Manager</b> <a href="mailto:David.hodges@bcc.net.au">David.hodges@bcc.net.au</a>	<b>IT Technician</b> <a href="mailto:Sean.raffaut@bcc.net.au">Sean.raffaut@bcc.net.au</a>	<ul style="list-style-type: none"> <li>• Information and Records management expertise – to assist in reviewing security and monitoring controls related to the breach (for example: access, recordkeeping practices) and aid recording the response to the data breach.</li> <li>• Information and Communication Technology (ICT) support/forensics support — this role can help establish the cause and impact of a data breach that involved ICT systems.</li> </ul>

# APPENDIX 3 – Notification Statement of an Eligible Data Breach

(e.g. risk of serious harm to individuals or school)  
Privacy Breach (Mandatory Reporting) 2018



**Bundaberg Christian College**  
Education with Wisdom

Contact Details: **Privacy Officer**  
**Bundaberg Christian College Ltd,**  
**234 Ashfield Road, Bundaberg QLD 4670.**  
**Ph: 07-4132 5800,**  
**Email: [privacy@bcc.net.au](mailto:privacy@bcc.net.au)**

Details of the “Eligible Breach”: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Remedial Action taken: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

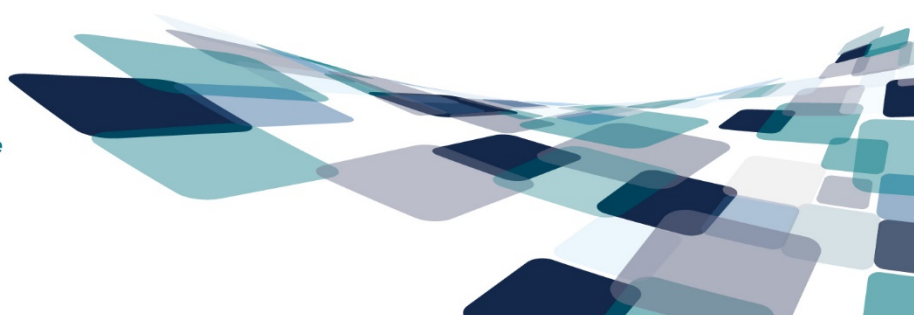
Nature of possible serious harm: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Who are the likely affected individuals? \_\_\_\_\_  
\_\_\_\_\_

How many individuals may be affected? \_\_\_\_\_

Is notification to individuals sufficient or does the College need to make a public notification via website or social media? \_\_\_\_\_  
\_\_\_\_\_

Future Actions: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



## APPENDIX 4

**Standard Collection Notice**

1. The College collects personal information, including sensitive information about students and parents or guardians 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 provide schooling to students enrolled at the College, exercise its duty of care, engage in marketing/fundraising and perform necessary associated administrative activities, which will enable students to take part in all the activities of the College.
2. Some of the information we collect 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 school require certain information to be collected and disclosed. These include relevant Education Acts, and Public Health [and Child Protection] laws.
4. Health information about students is sensitive information within the terms of the Australian Privacy Principles (**APPs**) under the *Privacy Act 1988*. We may ask you to provide medical reports about students from time to time.
5. The College may disclose personal and sensitive information for educational, legal, administrative, marketing and support purposes. This may include to:
  - other schools and teachers at those schools;
  - government departments (including for policy and funding purposes);
  - medical practitioners;
  - people providing educational, support and health services to the College, including specialist visiting teachers, [sports] coaches, volunteers, and counsellors;
  - providers of learning and assessment tools;
  - assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
  - 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 by law, including child protection laws, to disclose the information.
6. Personal information collected from students is regularly disclosed to their parents or guardians.
7. The College may use online or 'cloud' service providers to store personal information and to provide services to the College that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's server which may be situated outside Australia. Further information about the College's use of online or 'cloud' service providers is contained in the BCC Privacy Policy.
8. The College's Privacy Policy, accessible on the College's website, sets out how parents 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, where access may result in a breach of the College's duty of care to a student, or where students have provided information in confidence. Any refusal will be notified in writing with reasons if appropriate.
9. The College's Privacy Policy also sets out how parents and students can make a complaint about a breach of the APPs and how the complaint will be handled.
10. The College may engage in fundraising activities. Information received from you may be used to make an appeal to you. [It may also be disclosed to organisations that assist in the College's fundraising activities solely for that purpose.] We will not disclose your personal information to third parties for their own marketing purposes without your consent.
11. On occasions information such as academic and sporting achievements, student activities and similar news is published in College newsletters and magazines, on our intranet [and on our website]. This may include photographs and videos of student activities such as sporting events, College camps and College excursions. The College will obtain permissions [at enrolment] from the student's parent or guardian (and from the student if appropriate) if we would like to include such photographs or videos

[or other identifying material] in our promotional material or otherwise make this material available to the public such as on the internet.

12. We may include students' and students' parents' contact details in a class list and College directory.
13. If you provide the College with the personal information of others, such as doctors or emergency contacts, we encourage you to inform them that you are disclosing that information to the College and why.

## APPENDIX 5 – Disclosure Statement to Students and Parents

### **Counselling at Bundaberg Christian College – Things You Should Know**

The College provides counselling services for its students as part of its pastoral care program. These are provided through counsellors/chaplains employed by the College.

Students are encouraged to make use of these services if they need assistance. There are however a number of things that students and their parents should know before using the counselling service.

1. Students will attend counselling by invitation only and the decision to attend is the student's.
2. At any stage during the counselling service, the student is provided the chance to opt out.
3. It is the intention of the College, that parents/guardians be involved in supporting the counselling needs of their child/ren.
4. Records will be made of counselling sessions and because the counsellor/chaplain is an employee, those records belong to the College, not the counsellor/chaplain.
5. The College is very conscious of the need for confidentiality between counsellor/chaplain and student. However, at times it may be necessary for the Counsellor/Chaplain to divulge the contents of discussions or records to the Principal if the Principal or the Counsellor/Chaplain considers it necessary for the student's welfare to discharge the College's duty of care to the student.
6. It is also possible that the Principal may need to disclose aspects of discussions with counsellors/chaplains to others in order to assist the student.
7. Where a disclosure is made it would be limited to those who need to know, unless the student consents to some wider disclosure.

We emphasise that disclosures (if any) would be very limited. However, if a student is not prepared to use the counselling services on the basis set out above the student will need to obtain counselling services from outside the College.

## APPENDIX 6

**Alumni Association Collection Notice**

1. The College may collect personal information about you from time to time. The primary purpose of collecting this information is to enable us to inform you about our activities and the activities of the College and to keep alumni members informed about other members.
2. We must have the information referred to above to enable us to continue your membership of the BCC Alumni.
3. As you know, from time to time we engage in fundraising activities. The information received from you may be used to make an appeal to you. It may also be used by the College to assist in its fundraising activities. If you do not agree to this, please advise us now.
4. We may publish details about you in relevant publications, on social media and our/the College's website. If you do not agree to this, you must advise us now.
5. The BCC Privacy Policy, accessible on the College's website, contains details of how you may seek access to and correction of your personal information which the College has collected and holds, and how you may complain about a breach of the Australian Privacy Principles.
6. The College may use online or 'cloud' service providers to store personal information and to provide services to the College that involve the use of personal information, such as email services. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's server which may be situated outside Australia. Further information about the College's use of online or 'cloud' service providers is contained in the BCC Privacy Policy.
7. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the College and why.

## APPENDIX 7

**Employment Collection Notice**

1. In applying for this position, you will be providing the College with personal information. We can be contacted at 234 Ashfield Road, Bundaberg QLD 4670.
2. If you provide us with personal information, for example, your name and address or information contained on your resume, we will collect the information in order to assess your application for employment. We may keep this information on file if your application is unsuccessful in case another position becomes available.
3. The BCC Privacy Policy, accessible on the College's website, contains details of how you may complain about a breach of the Australian Privacy Principles and how you may seek access to and correction of your 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. Any refusal will be notified in writing with reasons if appropriate.
4. We will not disclose this information to a third party without your consent unless otherwise permitted. We usually disclose this kind of information to the following types of organisations such as support vendors that provide services around administration systems and agencies including Blue Card Services.
5. We may be required to conduct a criminal record check to collect information regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences under Child Protection laws. We may also collect personal information about you in accordance with these laws.
6. The College may use online or 'cloud' service providers to store personal information and to provide services to the College that involve the use of personal information, such as email services. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's server which may be situated outside Australia. Further information about the College's use of online or 'cloud' service providers is contained in the BCC Privacy Policy.
7. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the College and why.



## APPENDIX 8

**Contractor/Volunteer Collection Notice**

1. In offering, applying or agreeing to provide services to the College, you will be providing the College with personal information. We can be contacted 234 Ashfield Road, Bundaberg QLD 4670.
2. If you provide us with personal information, for example your name and address or information contained on your resume, we will collect the information in order to assess your application. We may also make notes and prepare a confidential report in respect of your application.
3. You agree that we may store this information for 5 years.
4. The BCC Privacy Policy, accessible on the College's website, contains details of how you may complain about a breach of the Australian Privacy Principles and how you may seek access to and correction of your 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. Any refusal will be notified in writing with reasons if appropriate.
5. We will not disclose this information to a third party without your consent unless otherwise permitted to. We usually disclose this kind of information to the following types of organisations such as support vendors that provide services around administration systems and agencies including Blue Card Services.
6. We may be required to conduct a criminal record check collect information regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences under Child Protection law. We may also collect other personal information about you in accordance with these laws.
7. The College may use online or 'cloud' service providers to store personal information and to provide services to the College that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's server which may be situated outside Australia. Further information about the College's use of online or 'cloud' service providers is contained in the BCC Privacy Policy.
8. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the College and why.