Ballarat Christian College

Policy Title	Privacy Policy
Date Policy Approved	July 2018
Policy Owner & Position	Principal
Team Responsible for Policy	Executive Leadership Team
Authorised by	Principal
Who is the Policy for?	Student, Staff and Parents
Version Control	V2
Statutory/Legislative Requirement	• *Privacy Act 1988 (Commonwealth)* • *Privacy Amendment (Notifiable Data Breaches) Act 2017* • Health Privacy Principles which are contained in the *Health Records Act 2001* (Vic)
Relevant cross references	• Enrolment Policy • First Aid Policy • Records Management Policy • Information Communication Technologies Policy • Vision, Purpose, Objects & Values, Child Safety Undertaking, Principles & Statement of Faith • Staff Code of Conduct
Include during Induction	Yes
Review Date	July 2020

Purpose of the Policy	This Privacy Policy sets out how Ballarat Christian College ('College') manages personal information provided to or collected by it.
Responsibility for Management of Policy	Business Manager
The Policy	The College is bound by the Australian Privacy Principles contained in the Commonwealth *Privacy Act 1988*. In relation to health records, the College is also bound by the Health Privacy Principles which are contained in the *Health Records Act 2001* (Vic). The College may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the College's operations and practices and to make sure it remains appropriate to the changing school environment. **What kinds of personal information does the College collect and how does the College collect it?** The College collects and holds personal data, relating to (but not limited to) health and other sensitive information, about: • Students and parents and/or carers ('Parents') before, during and after the course of a student's enrolment at the College, which may include: o Name, contact details (including next of kin), date of birth, gender, language background, previous school and religion;

- Parents' education, occupation and language background;
- Medical information (e.g. details of disability and/or allergies, absence notes, medical reports and names of doctors);
- Conduct and complaint records, or other behaviour notes, and school reports;
- Information about referrals to government welfare agencies;
- counselling reports;
- health fund details and Medicare number;
- any court orders;
- volunteering information; and
- photos and videos at College events;

- Job applicants, staff members, volunteers and contractors, which may include:
  - name, contact details (including next of kin), date of birth, and religion;
  - information on job application;
  - professional development history;
  - salary and payment information, including superannuation details;
  - medical information (e.g. details of disability and/or allergies, and medical certificates);
  - complaint records and investigation reports;
  - leave details;
  - photos and videos at College events;
  - workplace surveillance records;
  - work emails and private emails (when using work email address) and Internet browsing history; and

- Other people who come into contact with the College, including name and contact details and any other information necessary for the particular contact with the College.

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. On occasions people other than Parents and students may provide personal information.

Personal Information provided by other people: In some circumstances the College may be provided with personal information about an individual by a third party, for example a report provided by a medical professional or a reference from another school.

Exception in relation to employee records: Under the Privacy Act 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 employee. The College handles staff health records in accordance with the Health Privacy Principles in the Health Records Act.

How will the College use the personal information you provide?

The College will use personal information it collects from you for the primary purpose of the collection, and for such other secondary purposes that are related to the primary purpose and reasonably expected by you, or to which you have consented.

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, so that students are able to take part in all the activities of the College. This includes satisfying the needs of Parents, the needs of the students and the needs of the College throughout the whole period the student is enrolled at the College.

The purposes for which the College uses personal information of students and Parents may 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 and contractors: In relation to personal information of job applicants and contractors, the College's primary purpose of collection is to assess and (if successful) to engage the applicant or contractor.

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

- administering the individual's employment or contract
- insurance purposes;
- seeking donations and marketing for the College; and
- satisfying 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 associated activities, 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.

Parents, staff, contractors and other members of the wider College community may from time to time receive fundraising information. College publications, such as newsletters and magazines, which include personal information, may be used for marketing purposes.

To whom might the College disclose personal information which may then be shared?

The College may disclose personal information, including sensitive information, held about an individual for educational, administrative and/or support purposes. This may include:

- other schools and teachers at those schools;
- government departments (including for policy and funding purposes);
- medical practitioners;

- people providing educational, support and/or health services to the College, including (but not limited to) 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 and/or entities providing administrative and financial services to the College;
- recipients of College publications, such as newsletters and magazines;
- students' parents or carers;
- anyone to whom you authorise the College to disclose information; and
- anyone to whom we are required or authorised to disclose the information by law, including child protection laws.

Sending and storing information overseas: The College may disclose personal information about an individual to overseas recipients. However, the College will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

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 be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.

How does the College treat sensitive information?

'Sensitive information' means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information. It may also include health information and biometric information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is authorised/required by law.

Management and security of personal information

College staff are required to respect the confidentiality of students' and Parents' personal information and the privacy of individuals.

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

The Procedure	**Access and correction of personal information** Under the Commonwealth Privacy Act and the Health Records Act, an individual has the right to seek and obtain access to any personal information which the College holds about them and to advise the College of any perceived inaccuracy. Students will generally be able to access and update their personal information through their Parents, but older students may seek access and correction themselves. There are some exceptions to these rights set out in the applicable legislation. To make a request to access or to update any personal information the College holds about you or your child, please contact the College Privacy Officer. 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 the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal. **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 provided to parents will act as notice given to the student. Parents may seek access to personal information held by the College about them or their child by contacting the College Privacy Officer. However, there may be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the College's duty of care 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 warrant it. **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 College by emailing privacy@balcc.vic.edu.au or telephone (03) 5337 5900. The College will investigate any complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.

Data Breach Response Plan

In the event of a data breach, College personnel must adhere to the four phase 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.

Phase 1. Confirm, contain and keep records of the Data Breach and do a preliminary assessment

1. College personnel who become aware of the Data Breach or suspect a Data Breach has occurred must immediately notify the Business Manager. 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 Business Manager 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 College 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 Business Manager must consider if any of the affected individuals should be notified immediately where serious harm is likely.
5. The Business Manager must escalate **High Risk** and **Medium Risk** Data Breaches to the response team (whose details are set out at the end of this protocol).
6. If there could be media or stakeholder attention as a result of the Data Breach, it must be escalated to the response team.

Phase 2. Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely

1. The response team is to take any further steps (i.e. those not identified in Phase 1) available to contain the Data Breach and mitigate or remediate harm to affected individuals.
2. 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 establishing who the affected, or possibly affected, individuals are.

3. 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)
4. The response team should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise an EDB
5. 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.

Phase 3. Consider Data Breach notifications

6. 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.
7. 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 with the prescribed information and give a copy of the statement to the Information Commissioner.
8. 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.
9. 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.

Phase 4. Take action to prevent future Data Breaches

10. The response team must complete any steps in Phase 2 above that were not completed because of the delay this would have caused in proceeding to Phase 3.
11. The Business Manager must enter details of the Data Breach and response taken into a Data Breach log. The Business Manager must, every year, review the Data Breach log to identify any reoccurring Data Breaches.
12. The Business Manager 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 Protocol.
13. The Business Manager must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Response Protocol.
14. The Business Manager 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

The Response Team is to consist of the Business Manager, the ICT Manager, the Privacy Officer, and the Principal. They can be contacted via privacy@balcc.vic.edu.au or by phoning (03) 5337 5900.

Review	The College may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the College's operations and practices and to make sure it remains appropriate to the changing school environment.
Associated Policy & Procedure Documents	
Acknowledgement	The College acknowledges the permission of the Independent Schools Council of Victoria to use the content of their policy template in developing this document.

MANDATORY NOTIFICATION OF ELIGIBLE DATA BREACHES SUMMARY

MAINTAIN INFORMATION GOVERNANCE AND SECURITY

The College has an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

SUSPECTED OR KNOWN DATA BREACH

CONTAIN

Contain a suspected or known Data Breach where possible

ASSESS

The College 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 College has reasonable grounds to believe this is the case, then this is an **EDB** and it must notify individuals affected and the Information Commissioner. If it only has grounds to suspect that this is the case, then it must conduct an **assessment**. As part of the assessment, the College should consider whether **remedial action** is possible.

The College should consider adopting the OAIC's suggested a three-stage process:

Initiate: plan the assessment and assign a response 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 (and document this).

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

NO **IS SERIOUS HARM LIKELY** **YES**

NOTIFY

Where **serious harm is likely**, the College must prepare a statement for the Commissioner (a form available on OAIC website) that contains:

- The College's identity and contact details
- a description of the Data Breach
- the kind/s of information concerned
- recommended steps for individuals affected

The College 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 College's websiteand publicise it

The College can provide further information in their notification, such as an apology and an explanation of what they are doing about the Data Breach. **In some limited circumstances, an exception to the obligation to notify the individuals or the Commissioner may apply**

REVIEW

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

- Fully investigating the cause of the Data Breach
- Developing a prevention plan
- Conducting audits
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

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

- police or law enforcement
- other external or third parties (eg the ATO)
- The Australian Cyber Security Centre and related agencies
- professional bodies
- Credit card companies or financial services providers

This summary is a modified version of the OAIC Data Breach response summary available at www.oaic.gov.au/privacy- law/privacy-act/notifiable-data-breaches-scheme

DATA BREACH RISK ASSESSMENT FACTORS

Consider who the personal information is about	
Who is affected by the breach?	Are students, parents, staff, contractors, service providers, and/or other agencies or organisations affected? For example, a disclosure of a student's personal information is likely to pose a greater risk of harm than a contractor's personal information associated with the contractor's business.
Consider the kind or kinds of personal information involved	
Does the type of personal information create a greater risk of harm?	Some information, such as sensitive information (e.g. health records) or permanent information (e.g. date of birth) may pose a greater risk of harm to the affected individual(s) if compromised. A combination of personal information may also pose a greater risk of harm.
Determine the context of the affected information and the breach	
What is the context of the personal information involved?	For example, a disclosure of a list of the names of some students who attend the College may not give rise to significant risk. However, the same information about students who have attended the College counsellor or students with disabilities may be more likely to cause harm. The disclosure of names and address of students or parents would also create more significant risks.
Who has gained unauthorised access to the affected information?	Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or a party who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher at another school gains unauthorised access to a student's name, address and grades without malicious intent (eg if the information is accidentally emailed to the teacher), the risk of serious harm to the student may be unlikely.
Have there been other breaches that could have a cumulative effect?	A number of minor, unrelated breaches that might not, by themselves, create a real risk of serious harm, may meet this threshold when the cumulative effect of the breaches is considered. This could involve incremental breaches of the same College database, or known breaches from multiple different sources (eg multiple schools or multiple data points within the one school).
How could the personal information be used?	Consider the purposes for which the information could be used. For example, could it be used to commit identity theft, commit financial fraud, abuse the individual either physically or emotionally (including to humiliate the affected individual and social or workplace bullying)? For example, information on students' domestic circumstances may be used to bully or marginalise the student and/or parents. What is the risk of harm to the individual if the compromised information can be easily combined with other compromised or publicly available information?
Establish the cause and extent of the breach	
Is there a risk of ongoing breaches or further exposure of the information?	What is the risk of further repeat access, use or disclosure, including via mass media or online?

Is there evidence of intention to steal the personal information?	For example, where a mobile phone has been stolen, can it be determined whether the thief specifically wanted the information on the phone, or the phone itself? Evidence of intentional theft of the personal information (rather than just the device on which it is stored) can suggest an intention to cause harm, which may strengthen the need to notify the affected individual, as well as law enforcement.
Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?	Consider whether the information is rendered unreadable by security measures or whether the information is displayed or stored in way that renders it unusable if breached. If so, the risk of harm to the individual may be lessened.
What was the source of the breach?	For example, was it external or internal? Was it malicious or unintentional? Did it involve malicious behaviour or was it an internal processing error (such as accidentally emailing a student list to an unintended recipient)? Was the information lost or stolen? Where the breach is unintentional or accidental, there is likely to be less risk to the individual than where the breach was intentional or malicious.
Has the personal information been recovered?	For example, has a lost mobile phone been found or returned? If the information has been recovered, is there any evidence that it has been accessed, copied or tampered with?
What steps have already been taken to mitigate the harm?	Has the College fully assessed and contained the breach by, for example, replacing comprised security measures such as passwords? Are further steps required? This may include notification to affected individuals.
Is this a systemic problem or an isolated incident?	When identifying the source of the breach, it is important to note whether similar breaches have occurred in the past. If so, there may be a systemic problem with system security, or there may be more information affected than first thought, potentially heightening the risk.
How many individuals are affected by the breach?	If the breach is a result of a systemic problem, there may be more individuals affected than initially anticipated. The scale of the breach may lead to a greater risk that the information will be misused, so the response must be proportionate. Although it is vital to remember that a breach can be serious despite affecting only a small number of individuals, depending on the information involved.
Assess the risk of harm to the affected individuals.	
Who is the information about?	Some individuals are more vulnerable and less able to take steps to protect themselves (e.g. younger students, students with disabilities/special needs, vulnerable families/parents)
What kind or kinds of information is involved?	Some information, such as sensitive information (e.g. health records) or permanent information (e.g. date of birth) or a combination of personal information may pose a greater risk of harm to the affected individual(s) if compromised.
How sensitive is the information?	The sensitivity of the information may arise due to the kind of information involved, or it may arise due to the context of the information involved. For example, a list of the names of some students who attend the College may not be sensitive information. However, the same information about students who have attended the College counsellor or students with disabilities.

Is the information in a form that is intelligible to an ordinary person?	Examples of information that may not be intelligible to an ordinary person, depending on the circumstances may include: (i) encrypted electronic information; (ii) information that the College could likely use to identify an individual, but that other people likely could not (such as a student number that only the College uses – this should be contrasted to a student number that is used on public documents); and (iii) information that has been adequately destroyed and cannot be retrieved to its original form (such as shredded hard copy information).
If the information is not in a form that is intelligible to an ordinary person, what is the likelihood that the information could be converted into such a form?	For example, encrypted information may be compromised if the encryption algorithm is out-of-date or otherwise not fit for purpose and could be broken by a sophisticated attacker, or if the decryption key was also accessed or disclosed in the breach. Even where none of these concerns apply, the College may need to consider the likelihood of the encryption algorithm being broken in the long term.
Is the information protected by one or more security measures?	For example, are the systems on which the information is stored protected by intrusion detection and prevention systems, which identified the attack and stopped the attacker from accessing any information or copying the information?
If the information is protected by one or more security measures, what is the likelihood that any of those security measures could be overcome?	For example, could an attacker have overcome network security measures protecting personal information stored on the network?
What persons (or kind of persons) have obtained or could obtain the information?	Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher gains unauthorised access to a student's information without malicious intent, the risk of serious harm may be unlikely.
What is the nature of the harm that could result from the breach?	Examples include identity theft, financial loss, threat to physical safety, threat to emotional wellbeing, loss of business or employment opportunities, humiliation, damage to reputation or relationships, or workplace or social bullying or marginalisation. For example, information on students' domestic circumstances may be used to bully or marginalise the student and/or parents.
In terms of steps to mitigate the harm, what is the nature of those steps, how quickly are they being taken and to what extent are they likely to mitigate the harm?	Examples of steps that may remediate the serious harm to affected individuals might include promptly resetting all user passwords, stopping an unauthorised practice, recovering records subject to unauthorised access or disclosure or loss, shutting down a system that was subject to unauthorised access or disclosure, or remotely erasing the memory of a lost or stolen device. Considerations about how quickly these steps are taken or the extent to which the steps taken are remediating harm will vary depending on the circumstances.
Any other relevant matters?	The nature of other matters that may be relevant will vary depending on the circumstances of the College and the Data Breach.
Assess the risk of other harms.	
What other possible harms could result from the breach, including harms to the College or AIS/CEC?	Examples include loss of public trust in the College or AIS/CEC, damage to reputation, loss of assets (e.g. stolen laptops), financial exposure (e.g., if bank account details are compromised), regulatory penalties (e.g., for breaches of the Privacy Act), extortion, legal liability, and breach of secrecy provisions in applicable legislation.