Coast
CHRISTIAN SCHOOL

Privacy Policy

Foundation for Life

Table of Contents

1. Purpose

Coast Christian School (the School) is committed to:

- respecting privacy;
- ensuring the personal information provided to us and collected by us is managed and retained in a secure manner; and
- ensuring the personal information entrusted to us is used primarily for the purpose of operating the School and discharging our responsibilities as a School.

Additionally, the School is subject to the Privacy Act 1988 (Cth) (the Act) and the 13 Australian Privacy Principles (APPs).

This policy sets out how the School fulfils our commitment to being open and transparent concerning the manner in which we manage personal information (**APP 1**).

2. Scope

This policy applies to all staff, contractors and volunteers at the School.

The protections of the policy extend to the personal information of all stakeholders of the School including students, parents and others where relevant.

3. Distribution of this policy

This policy is to be provided to all staff, contractors and volunteers at the School at the time of their engagement with the School. Staff are to be given refresher training at appropriate intervals.

This policy is available on the School's website (**APP 1**) and upon request.

4. Definitions

Australian Privacy Principles (APPs) – principles for managing personal information set out in the Privacy Act 2002 (Cth).

Personal Information – information or an opinion, whether true or not, about an individual whose identity is apparent, or can reasonably be inferred from, the information or opinion, whether the information is recorded in a material form or not. It includes all personal information, regardless of its source – which includes sensitive information.

Examples of personal information include:

- Particulars of students (including name, contact details, date of birth, gender, language, previous school, religion etc) and their parents
- Health and medical information (health issues, disabilities, medical reports etc)
- Academic information (test results, prior school records etc)

- Court orders (eg AVO's and Family Law orders etc)
- Photographs, videos and other records of school activities
- Particulars of staff, volunteers and contractors (eg identification, references, qualifications etc)
- Particulars of other people in the School community (eg relatives and friends of students, educational presenters and other providers)
- Sensitive information (see below)
- Health information (see below)

Sensitive Information (a subset of Personal Information) – personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's health, racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, membership of a professional or trade association, philosophical beliefs, membership of a trade union, sexual orientation or practices, or criminal record. Sensitive information includes Health Information.

Health Information (a subset of Sensitive Information) – information or an opinion about: the health or disability (at any time) of an individual; an individual's expressed wishes about the future provision of health services to him/ her; a health service provided, or to be provided, to an individual.

5. Related policies/documents

- Complaints and Grievances Policy
- Whistleblower Policy

6. Responsibilities

The School Board is responsible for approving this policy and amendments of it.

The School Principal is responsible for implementing this policy organisation-wide.

All staff, contractors and volunteers are to abide by this policy when dealing with personal information collected by the School.

7. Exclusions from this policy

Employment records

Employee records and acts done by the School as the employer of staff - if directly related to a current or former employment relationship - are generally excluded from the application of the Privacy Act and this policy.

Examples of this type of information include the terms and conditions of employment, personal contact details, performance and conduct and salary details.

The School may access and use personal information about employees as appropriate.

Other contexts

Some contexts will require the School to manage personal information otherwise than covered this policy, for example, where other legislative/regulatory requirements or legal obligations take precedence eg child protection investigation processes, whistle-blower scenarios, etc. In particular, Part 5A of the Education Act 1990 (NSW) allows government and non-government schools in NSW to exchange information that is relevant to the assessment and management of health and safety risks to students or staff arising from a student's history of violent behaviour.

8. Soliciting of information

Generally

The School solicits (**APP 3**) personal information including (but not limited to) information, about:

- Students and parents/ guardians before, during and after the course of a student's enrolment at the School (including sensitive and health information)
- Job applicants, staff members and their families where relevant
- Volunteers and contractors
- Other individuals who come into contact with the School

Where possible, the School collects information from the individual concerned.

Consent

Due to the age of the students at the School (ie preparatory to Year 6) the School will require parental consent in relation to privacy issues and will treat consent given by the parents as consent given on behalf of the student.

9. Unsolicited personal information

If we receive unsolicited personal information (**APP 4**), we will destroy it unless we are permitted to hold the information and it is needed to carry out our functions or fulfil our duty of care to students or staff.

10. Advice to information providers

Before information is provided or as soon as practicable after it is provided, the School will notify the individual to whom the information relates of the following:

- The fact that information is being collected
- The purpose for which the information is being collected
- The intended recipients of the information
- Whether the supply of information by the individual is required by law, or is voluntary; and any consequences for the individual if the information is not provided, or part not provided
- The existence of any right of access to, and correction of, the information

This information is outlined in the School's Standard Collection Notice (**APP 5**).

11. Use of personal information

The School will use personal information (**APP 6**) provided to it for the primary purpose of collection (eg assess suitability for enrolment or employment etc); and for related secondary purposes which may be reasonably expected, or to which you have expressly consented (eg to enable the School to fulfil its objectives, functions and powers).

Students and Parents/ Guardians

The School's primary purpose of collection of personal information is to enable the School to provide schooling for the student. This includes satisfying both the needs of parents/ guardians, the needs of the student and the needs of the School throughout the whole period the student is enrolled at the School.
The purposes for which the School uses this personal information include:

- To keep parents informed about matters relating to the child's schooling, through correspondence, reports, newsletters and magazines
- The student's educational, social and medical well-being
- Celebrating the efforts and achievements of students
- Day-to-day administration
- Seeking donations for the School
- Conducting marketing and fundraising for the School (APP 7)

- To satisfy the School's legal obligations and allow the School to discharge its duty of care
- Complying with Federal and State reporting requirements
- Investigating incidents or defending any legal claims against the School, its services or staff

Where the School requires personal information about a pupil or parent/ guardian which is not provided, the School may not be able to enrol or continue the enrolment of the student or permit the student to take part in a specific activity.

Job applicants, staff members and contractors

The School requests personal information for:

- Assessing suitability for employment, to engage an employee or contractor
- Administration of the individual's contract or employment
- Insurance purposes, such as public liability or Work Cover
- Satisfying the School's legal obligations, for example in relation to child protection legislation
- Investigating incidents, or defending legal claims about the School, its services or staff
- Seeking donations, and marketing of the School

(However note also the exception regarding employment records referenced in this policy.)

Volunteers

The School obtains personal information about volunteers who assist the School in its functions, or conduct associated activities, to enable the School and the volunteers to work together.

Marketing and Fundraising

The School treats marketing, and seeking donations for the future growth and development of the School, as an important part of ensuring that the School continues to be a quality learning environment in which both students and staff thrive.
Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

12. Disclosure of Personal Information

Generally

For the educational, administrative and supportive purposes, the School may disclose personal information (**APP 6**) held about an individual to:

- Another schools/teachers
- Assessment and educational authorities eg NESA and NAPLAN
- Government departments

- Medical and allied health practitioners
- Service providers to the School eg music tutors; finance services
- Recipients of School publications, such as newsletters and magazines; School Directory
- Parents of the student enrolled; unless a Court Order limiting access by one parent is received by the School
- Anyone as authorised by the parents/ guardians of the student
- Any individual or organisation as required by law

Sensitive information and Health information is only disclosed for the purpose for which it was provided or where otherwise allowed by law.

Students

The School will refer any notices in relation to the personal information of a student to the student's parents.

Notice given to the parents will act as notice given to students.

13. Christian Schools Australia Schools

Each school within the Christian Schools Australia umbrella - being legally related to each of the other schools as member schools - may share personal information (but not sensitive or health information) with other CSA schools. Other CSA schools may then only use this personal information for the purpose for which it was originally collected. This allows schools to transfer information between them, for example, when a pupil transfers from a Christian school to another CSA school.

14. Cross-border disclosure

The School will not send personal information about an individual outside Australia (**APP 8**) except as follows:

- Where consent of the individual (unless already implied) is given eg to facilitate arrangements for an overseas trip for students
- Where data is stored 'in the cloud' with a reputable provider (eg Microsoft Office 365) whose data servers may exist outside Australia, and with appropriate security features in place (eg dual authentication etc)

15. Withdrawal of Consent and Do Not Publish

Where possible, the School creates opportunities for parents to choose for their child's or family's information not to be published, for example photos/ videos; School Directory; use of student's work etc. Parents may inform the School during the enrolment process, at annual update of information, or at any other time by advising the School in writing of withdrawal of consent.

Where appropriate and reasonably practicable, we give individuals the option of not identifying themselves or to use a pseudonym instead. (**APP 2**)

16. Quality of personal information

The School takes all reasonable steps to make sure that the personal information it collects and stores is of sound quality (**APP 10**), ie accurate, up-to-date, complete, relevant and not misleading.

17. Accessing and correction of personal information

An individual has the right under this policy to obtain access to any personal information which the School holds about them (**APP 12**); and to advise the School of any perceived inaccuracy and to seek correction to their information (**APP 13**).

Students (due to their age being a preparatory-year 6 school) are able to access and update their personal information through their parents only. Personal information may be accessed or updated by contacting the School in writing. The School will require verification of identity and details of what information is required. If the information sought is extensive, the School may require a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested.

Access to personal information will be denied in all appropriate cases such as where:

- It would pose a serious or imminent threat to the life or health of an individual
- Release may result in a breach of the School's duty of care to the student
- It would have an unreasonable impact on the privacy of other individuals
- It is likely to prejudice the prevention, detection, investigation, prosecution or punishment of an unlawful activity, the activities of a law enforcement agency, or legal proceedings
- The request is frivolous or vexatious
- The information relates to existing or anticipated legal proceedings between the parties, and the information would not be accessible through legal procedures
- Providing access would be unlawful
- Denying access is required or authorized by or under law

If the School cannot provide access to the information required, the School may be able to provide a format of information that protects the privacy of other individuals. A written notice explaining the reasons for a refusal will be provided.

18. Storing personal information

We will store personal information securely so that it can only be readily accessed by a staff member with a legitimate reason for using it, and it is protected from interference, misuse, loss or unauthorized access.

Personal information about students, parents or staff that we keep in databases will be protected from general access by effective security arrangements such as passwords so that only those with a legitimate reason can gain access to the information relevant to them. Workstations and software applications such as email will log off after a predetermined period of inactivity to prevent unauthorised access when they are unattended.

Personal information on paper will be kept in locked storage and be protected by any other security measures appropriate to maintaining the required level of confidentiality and privacy. Documents with personal information must not be left visible and unattended in work areas.

19. Security of personal information

The School retains personal information securely (**APP 11**) and has in place steps to protect the personal information the School 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, and restricting access to relevant people in areas where personal information is stored.

The School's staff are required to respect the confidentiality of students' and parents' personal information, and the privacy of individuals.

20. Information no longer needed

The School will not store personal information longer than necessary.

When personal information is no longer needed for the purpose for which it was collected, we will destroy it (or de-identify it).

21. Government related identifiers

The School does not adopt, use or disclose government related identifiers (**APP 9**) which are a letter, number, symbol used to identify an individual or verify their identity, including:

- Medicare numbers
- Centrelink reference numbers
- Driver's licence details
- Australia Passport numbers

22. Breach of privacy

A breach of privacy protection may result from mishandling personal information.

A data breach concerns the loss of security of personal information and involves unauthorised access to, or accidental/intentional disclosure of, personal information; or the loss of personal information where the loss is likely to result in unauthorised access or disclosure.

Causes of a breach may include malicious acts of third parties; human error; systems failure; or failure to follow information handling or data security measures resulting in accidental loss, access or disclosure.

If a data breach is suspected, or confirmed, the School shall take remedial action as soon as is practicable to contain and limit the data loss or access; and to minimise the chance of serious harm to any individual affected by the breach. Where appropriate, the School shall notify relevant persons of the breach and remedial actions taken. The School shall investigate the circumstances, and take steps to address any systemic issues to improve data security.

23. Notifiable Data Breach (NDB) Scheme

The Notifiable Data Breach (NDB) scheme compels organisations to notify individuals and the Office of the Australian Information Commissioner and Privacy Commissioner (OAIC) in the event of a personal information data breach likely to result in 'serious harm' (ie an 'Eligible Data Breach').

'Serious harm' includes psychological, emotional, physical, reputational or other forms of harm.

An 'Eligible Data Breach' is:

- a situation where there is unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information, held by an entity
- which is likely to result in serious harm to one or more individuals, and
- the entity has not been able to prevent that likely risk of serious harm with remedial action.

We have 30 days to assess whether a data breach is likely to result in serious harm. If we are successful in reducing the level of harm below serious or if the breach is assessed at a level below serious, we are not required to notify you.

If there is an Eligible Data Breach, we must:

- prevent further loss of, or access to, the data as soon as is practicable;
- notify all affected individuals, directly or indirectly, as soon as is practicable;
- prepare a statement of prescribed information regarding the Eligible Data Breach for submission to the OAIC, and make the affected individuals aware of the contents of the statement; and
- take action to address the cause/s of any data breach against further loss of information.

The OIAC's role is to:

- receive notifications of eligible data breaches
- encourage compliance with the NDB scheme, including by handling complaints, conducting investigations and taking other regulatory action
- offer advice and guidance to regulated organisations
- provide information to the community about the operation of the NDB scheme.

24. Complaints

Any concerns about the way the School has handled information, or a data breach, should be made in writing and directed to the Principal who will investigate the complaint and notify you of the decision as soon as practicable.

If you are not satisfied with the decision, you may direct a complaint to the School Board via the School's Complaints Handling Policy.

Complaints may also be directed to the OAIC on 1300 363 992 or as per their website (oaic.gov.au).

25. Enquiries

For further information about the way we manage personal information, please contact us:

The Principal
Coast Christian School
PO Box 6064
Kincumber NSW 2251
02 4368 3377

26. Legislative references

Privacy Act 1988 (Cth)

Health Records and Information Privacy Act 2002 (NSW)

Education Act 1990 (NSW)