NAZARETH COLLEGE

PRIVACY POLICY

Developed: 2002
Responsible Officer: Compliance Officer
Ratified by Board of Management: March 2020
Last Reviewed: March 2021
Due for Review: March 2023

Nazareth College Privacy Policy

Document Details

Document Name	Privacy Policy
Document created by	Principal Compliance
Document Approval	Leadership Team

Document Management

Relevant to	All Staff, Volunteers, Contractors, Parents/Guardians/Carers and Students
Related documents	• Data Breach Policy and Response 2020 • Staff Digital Device User Agreement 2021 • Student Digital Learning User Agreement 2021 • Enrolment Policy 2020 • Counselling Policy 2018 • Feedback Policy 2021 (Pending) • Complaints Policy 2020 • Child Information and Family Violence Information Sharing Policy 2021 (Pending)
Related Legislation	• Privacy Act 1988 (Cth) • Health Records Act 2001 (Vic) • Australian Privacy Principles • Health Privacy Principles • Notifiable Data Breach Scheme 2020 • Australian Education Regulation 2013 • Australian Education Act 2013 • Nationally Consistence Collection of Data (NCCD) • section 41ZA of the Child Wellbeing and Safety Act 2005 • Part 5A of the Family Violence Protection Act 2008,
Review	The Policy shall be reviewed every 1-3 years or as required (in the event of any information or incident that would warrant a review including any legislative or organisational change)

Change History

Author	Date	Description	Version
G. Giese	2002	Original Privacy Policy created, reviewed and approved	V1
T. Burnett	03/03/2020	Privacy Policy rewritten to align with VRQA requirements	V2
T. Burnett	02/03/2020	Privacy Policy ratified by the board	V2
T. Burnett	03/09/2020	Privacy Policy communicated to all staff and published to website	V2
T Burnett	11/03/2021	Privacy Policy amended to include CISS, FVISS and MACS requirements	V3
T Burnett	19/03/2021	Privacy Policy ratified by leadership	V3

PURPOSE

The Privacy Policy sets out how Nazareth College manages personal information provided to the College or collected by it.

The College is bound by the Australian Privacy Principles (APPs) contained in the Commonwealth *Privacy Act 1988*. In relation to health records, the College is also bound by the *Health Records Act 2001* (Vic) and the Health Privacy Principles in that Act.

Nazareth 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 ensure it remains appropriate to the changing school environment.

WHAT KIND OF PERSONAL INFORMATION DOES NAZARETH COLLEGE COLLECT AND HOW DOES THE COLLEGE COLLECT IT?

The type of information the school collects and holds includes, but is not limited to, personal information, including health and other sensitive information, about:

1. **Students and parents and/or guardians before, during and after the course of a student's enrolment at the College including**:

- Name, contact details (including next of kin), date of birth, country of birth, citizenship, gender, language background, previous school and religion
- Parents' education, occupation, language and citizenship background
- Medical information (e.g. details of disability and/or allergies, and details of any assistance the student receives in relation to those disabilities, medical reports, names of doctors)
- Conduct and complaint records, or other behaviour notes, school attendance and school reports both from the school and from other schools
- Information about referrals to government welfare agencies
- Counselling reports
- Health fund details and Medicare number
- Payment information / financials;
- Any court/parenting orders;
- Volunteering information (including Working with Children Checks);
- Photos and videos at College events.

2. **The personal information of Job applicants, Staff Members, Volunteers, Visitors and Contractors, including:**

- 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;
- Work emails and private emails (when using work email address) and internet browsing history;
- Police Record checks; (non-teaching staff)
- Workplace surveillance information;

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

4. 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 provided by you

Nazareth will generally collect personal information held through a number of ways listed below, but not limited to:

- Through the completion of forms
- Face-to-face meetings or interviews
- Emails, telephone calls, invoices or consent forms
- School-controlled social media
- Letters to the School

- Website notification or online tools such as apps and other software used by the school
- Through any CCTV cameras located at the school
- Photography and videography
- People (other than parents and students) provide personal information and where this is the case, this information may also be collected

On occasions people other than parents and students (such as job applicants and contractors) provide personal information to the school

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

- Academic records and/or achievement levels;
- Information that may be relevant to assisting Nazareth college meets the needs of the student including any adjustments.
- Child Information and Family Violence Information Sharing Scheme requests

Personal information collected about other people
In some circumstances the school may collect personal information about other people when (but not limited to):

- Assessing applicant's suitability for employment or volunteering
- Administering employment or volunteering placement
- Public liability or WorkCover insurance purposes
- Employment and contractual obligations
- Occupational Health and Safety laws and/or when required to investigate incidents
- Legal claim responses

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 2001 (Vic.).*

Anonymity
The College needs to be able to identify individuals with whom it interacts and to collect identifiable information about them to facilitate the delivery of schooling to its students and its educational and support services, conduct the job application process and fulfil other obligations and processes. However, in some limited circumstances, some activities and interactions with the College may be done anonymously, where practicable, which may include making an inquiry, complaint, a whistle-blower report or providing feedback.

HOW WILL NAZARETH COLLEGE USE THE PERSONAL INFORMATION YOU PROVIDE?
The school will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected by you, or to which you have consented. This includes satisfying the needs of parents and/or guardians (described as 'parents' throughout this document), the needs of the student and the needs of the school throughout the whole period the student is enrolled at the school. For more information on the School's Collections Notice, please refer to it.

Students and Parents:
In relation to personal information of students and parents, the school's primary purpose of collection is to enable the school to provide educational and support services to students enrolled at the school, exercise the school's duty of care and perform necessary associated

administrative activities which will enable students to take part in all the activities of the school, including but not limited to:

- Delivering a high quality, relevant and contemporary educational experience
- Keeping parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines
- Day-to-day administration
- Looking after students' educational, social, and medical wellbeing
- Seeking donations and marketing for the school
- Managing the physical and electronic security of the school
- Satisfying the school's legal obligations and allow the school to discharge its duty of care
- Taking reasonable steps to reduce risk of harm to students, staff, parents or visitors
- Making reasonable adjustments by providing support to students with disabilities
- Providing a safe and secure workplace
- Ensuring effective management, resourcing, administration, statutory duties, planning, funding, monitoring, regulating, evaluating policies and processes, complying with reporting, mitigating risks, investigating incidents and responding to any legal claims
- Seeking feedback from students and parents on school performance and improvement, including through school improvement surveys
- Satisfying the School service providers' legal obligations, including the Catholic Education Commission of Victoria Ltd (CECV) and the Melbourne Archdiocese Catholic Schools Offices
- When necessary to lessen or prevent a serious threat to a person's life, health, safety or welfare, the public's health, safety or welfare and/or for contact tracing purposes

In some cases where the school requests personal information about a student or parent/guardian and if the information requested 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 particular activity.

Job applicants and contractors

In relation to the 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, which includes, but not limited to:

- Administering the individual's employment or contract, as the case may be;
- For insurance purposes;
- Seeking donations and marketing for the College;
- Satisfying the school's legal obligations (i.e. 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, to enable the College and the volunteers to work together, to confirm their suitability and to manage their visits.

Psychologist

The school has employed a School Psychologist and occasionally contracts with external providers to provide counselling services and/or assessment services for some students. The Principal may require the School Psychologist to inform them or other teachers or non-teachers of any issues the Principal and the School Psychologist believe may be necessary for the school to know for the wellbeing or development of the student who is counselled or other students at the school.

Parish

The College may disclose limited personal information to the feeder parishes to facilitate religious and sacramental programs, and other activities such as fundraising.

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 school's fundraising, for example, the Nazareth College Community Association (NCCA).

Parents/guardians, staff, contractors and other members of the wider College Community may from time to time receive fundraising information. College publications, like newsletters and magazines, which include personal information and sometimes people's images, may be used for marketing purposes.

Information Sharing Entities
Organisations and services prescribed under the Child Information Sharing Scheme (CISS) and the Family Violence Information Sharing Scheme (FVISS).

Unsolicited information
We may receive information that we have taken no active steps to collect. If this is the case and if permitted/required by law, we may keep records of this information. However, we may destroy the information when practicable, lawful or when it is reasonable.

WHO MIGHT THE COLLEGE DISCLOSE PERSONAL INFORMATION TO AND STORE YOUR INFORMATION WITH?
The school may disclose personal information, including sensitive information, held about an individual for educational, administrative and support purposes. This may include but is not limited to:

- College service providers which provide educational, support and health services to the College, (either at the school or off campus) including the Catholic Education Commission of Victoria Ltd (CECV), Melbourne Archdiocese Catholic Schools (MACS) Offices, specialist visiting teachers, volunteers, counsellors, sports coaches and providers of learning and assessment tools;
- Third party service providers that provide online educational and assessment support services, services in relation to school improvement surveys, document and data management services, or applications to schools and school systems including Synergetic, Simon, PAM, Zoom, Cyberhound, Microsoft and Google's G Suite For Education and Outlook where necessary, to support the training of selected staff in the use of these services;, including for the purposes of facilitating access, and where necessary, to support the training of selected staff in the use of these services
- CECV, and MACS offices, to discharge its responsibilities under the Australian Education Regulation 2013 (Regulation) and the Australian Education Act 2013 (Cth) (AEAct) relating to students with a disability.
- Other third parties which the school uses to support or enhance the educational or pastoral care services for its students or to facilitate communications with Parents/guardians
- Another school, including its teachers, to facilitate the transfer of a student;
- Federal and State Government departments and agencies;
- Health service providers;
- Recipients of College publications, such as newsletters and magazines;
- Students, parents or guardians and their emergency contacts;
- Assessment and educational authorities including the Australian Curriculum Assessment and Reporting Authority;
- Anyone you authorise the College to disclose information to;
- Anyone whom we are required or authorised to disclose the information to by law, including child protection laws.
- Information Sharing Entities prescribed under the Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS).
- Another school for the purpose of transferring schools which enables the next school to continue to provide education, support, health and wellbeing and/or fulfil legal requirements

- NAPLAN results when students transfer schools or when required to evaluate a school's education program
- Medical practitioners
- If/when necessary to mitigate health, safety or wellbeing risks
- When required by law such as duty of care, anti-discrimination laws, OHS laws, reporting obligations, court orders or Victorian Police warrants
- Investigate, report or prevent activities or incidents, misconduct, criminal offence, legal claims or on behalf of a law enforcement agency
- School statistics, research or reporting requirements
- Responding to complaints received from students, parents/guardians, staff, contractors, volunteers or complaints received from the community
- 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 allowed by law

Nationally Consistent Collection of Data on School Students with Disability
The College is required by the Federal *Australian Education Regulation (2013)* and *Australian Education Act 2013* (Cth) (AE Act) to collect and disclose certain information under the *Nationally Consistent Collection of Data* (NCCD) on students with a disability. The College provides the required information at an individual student level to the MACS Offices and the CECV, as an approved authority. Approved authorities must comply with reporting, record keeping and data quality assurance obligations under the NCCD. Student information provided to the Federal Government for the purpose of the NCCD does not explicitly identify any student.

Child Information and Family Violence Information Sharing
The Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS) explicitly recognise that a child's safety and wellbeing, and family violence victim survivor safety take precedence over any individual's privacy. Therefore, consent to collect or disclose personal information is not required under the following circumstances:

- Information Sharing Entities prescribed under CISS and FVISS.
- When assessing or managing the risk of family violence to a child
- To promote and protect the wellbeing and safety of a child
- When information relates to a perpetrator of family violence - for assessing or managing family violence risk
- Risk assessment entities prescribed under FVISS for sharing information to assess the risk of family violence and for managing the risk of family violence once risk has been established

Sending and storing information overseas
The school may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school immersion programs. However, the school will not send personal information about an individual outside Australia without obtaining the consent of theindividual; or otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

The school may from time to time use the services of third party online service providers including for the delivery of services and third party online applications, or Apps relating to email, instant messaging and education and assessment, such as Google's G Suite and Outlook) which maybe accessible by you. Some personal information, including sensitive information may be collected and processed or stored by these providers in connection with these services. These online service providers may be located in or outside Australia.

School personnel, the school's service providers, CECV and its service providers, may havethe ability to access, monitor, use or disclose emails, communications, documents and associated administrative data for the purposes of administering the system and services ensuring their proper use.

The school makes reasonable efforts to be satisfied about the security of any personal information that may be collected, processed and stored outside Australia, in connection with any cloud and third party services and will endeavour to ensure the cloud is located in countries with substantially similar protections as the APPs.

The country in which the servers of cloud service providers and other third-party service providers may be located in Australia or overseas. Where personal and sensitive information is retained by a cloud service provider on behalf of CECV to facilitate Human Resources and staff administrative support, this information may be stored on servers located in or outside Australia.

The countries in which the servers of cloud services provide, and other third-party service providers are located, may include:

Americas

- Berkeley County South Carolina;
- Council Bluffs Iowa;
- Douglas County Georgia;
- Jackson County Alabama;
- Lenoir, North Carolina;
- Mayes County;
- Oklahoma;
- Montgomery County;
- Tennessee;
- Quilicura Chile;
- The Dalles Oregon;

Asia

- Changhua County;
- Taiwan Singapore;

Europe

- Dublin Ireland;
- Eemshaven Netherlands;
- Hamina Finland;
- St Ghislaine Belgium.

HOW DOES THE COLLEGE TREAT SENSITIVE INFORMATION?

In referring to 'sensitive information', the school means information relating to a person's:

- Racial, ethnic origin, political opinions, religion and/or philosophical beliefs
- Trade union/other professional or trade association membership
- Sexual orientation or practices
- Criminal record
- Health information or biometric information

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 allowed by law.

Management and Security of Personal Information

School staff, the school’s service providers and contractors are required to protect personal and sensitive information that is under their control. Access to personal or sensitive information by staff is limited to that required by their role. Where personal data is required to be transmitted or stored in a location other than the school’s main campus, this data will be accessed only via secure, encrypted channels and accessible only to authorised personnel. Physical records are stored in secure, locked files and all keys issued are recorded on the School’s Key Register.

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

The school 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. This includes responding to any incidents which may affect the security of the personal information it holds. If we assess that anyone whose information is affected by such a breach is likely to suffer serious harm as a result, we will follow the School's Notifiable Data Breach Policy which includes notifying the person/people of the data breach and report the breach to the Office of the Australian Information Commissioner.

It is recommended that students, parents and the College Community adopt secure practices to protect themselves which include but are not limited to:

- Ensuring that all passwords are strong and regularly updated
- Ensuring Log in details are kept secure.
- Not sharing personal information with anyone without first verifying their identity and organisation.

if a student, parent or a member of the schoolcommunity believe that their personal information has been compromised, please let the school know immediately

Storing and Securing Information

The school takes reasonable steps to protect information from misuse and loss and from unauthorised access, modification and disclosure. The School stores all paper and electronic records securely. All school records are securely disposed of or transferred to internal archives. When using software and contracted service providers to manage information, these are assessed in accordance with the appropriate department process or role description.

School publications

On occasions, information (including images or video) such as academic and sporting achievements, camps and excursions, other student activities and similar news is published in the School Newsletters, magazines, social media and on the school's Parent Portal. As part of the Business Terms, parents give their consent for student work, photographs and/or names to appear in publications. If parents wish to revoke this consent, they must advise the school by completing the photo/video permission form.

Google Drive / Microsoft Teams

Google Drive and Microsoft Teams is an online file storage system provided to the school. It is school policy that certain information is not stored in Google Drive. This includes, but is not limited to:

- Information about the wellbeing of students
- Medical information
- Financial information, including credit card or bank account details
- Advisory Council Papers, including papers of Committees of the Board
- Usernames, passwords or other access information
- Information pertaining to legal matters
- Records of employment
- Student, staff or parent images

Auditing and review of access

The School's ICT Department may from time to time be required to audit or review access records or other metadata to ensure relevant compliance to the School's Privacy Policy. ICT staff will not access any data unless requested by: Business Manager, Deputy Principals and/or the Principal.

Third-party access

There may be circumstances where it is necessary for data held in the name of an individual such as email or files stored on network drives, hard drives, Microsoft Teams, SharePoint or

Google Drive, to be accessed bythe Schools' ICT Department and when this is required, written authorisation is required from:

- Deputy Principal (Staff and Students) – in the case of students
- Business Manager or Deputy Principal (Teaching and Learning) - in the case of staff
- Principal (in the case of members of the Leadership Team and incident management)

Closed Circuit Television

The school operates a number of closed-circuit television cameras to monitor and manage the physical security of our campus. These cameras are located at key locations, predominantly externally. Cameras are not located in classrooms, staff offices, toilets or change rooms or the school's sickbay. Notices of the presence of the camera system are located at each major entrance to the property. Cameras record 24 hours per day, seven days per week and recordings are retained for a period of time to allow for the review of historical incidents as required. After a period of time has passed, the footage is automatically deleted. Live monitoring of some cameras also takes place and screens are located in various locations.

Access and Correction of Personal Information

The school respects every parent's right to make decisions concerning their child's education.

Generally, the school will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. The school 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.

Under the Commonwealth Privacy and the Health Records Act, an individual has the right to seek and obtain access to any personal information and health records respectively which the College holds about him/her and to advise the College of any perceived inaccuracy. Students will generally be able to access and update their personal information through their parents/guardians, but older students may seek access and correction themselves.

Parents may seek access to personal information held by the school about them or their child by contacting the School Principal or College Registrar by telephone or in writing. 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.

However, there will be occasions when access is denied. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal. There may be circumstances where the reason for refusal is not provided. 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 school's duty of care to the student.

The school may, at its discretion, on the request of a student grant that student access to information held by the school 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 about you, or wish to complain that you believe that the College has breached The Australian Privacy Principles, please contact the College Principal via email principal@nazareth.vic.edu.au or by phone 9795 8100. 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.

If you are not satisfied with the College's decision you may make a complaint to the Office of the Australian Information Commissioner (OAIC) whose contact details are

GPO Box 5218, Sydney NSW 2001
Telephone: 1300 363 992
Website www.oaic.gov.au