Nowra Christian School
Grow up into Christ

194 Old Southern Rd, SOUTH NOWRA
PO Box 620 NOWRA NSW 2541
E office@ncs.nsw.edu.au
P +61 02 4422 1199

NCS Privacy Policy & Procedure

Adopted: May 2019
Last amended: May 2019
Next review: June 2022

Rationale

As an organisation that values Christian community, NCS recognises its responsibilities to safely manage the collection, storing and sharing of personal information. Personal information (of staff, students, families and any entity connected with the School), will be held in strictest confidence and will only be used for the purposes for which it was collected.

This policy statement is based on the Australian Privacy Principles in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* which amends the *Commonwealth Privacy Act 1988*. Schools are also bound by the *Health Records and Information Act 2002*. This policy exists in order to demonstrate our firm commitment to protecting personal and sensitive information.

Definitions

Personal Information- information about an individual (whether in written, photographic or otherwise) which, when combined with other information (which may not be controlled by the same entity), identifies an individual or renders the individual reasonably identifiable.

Sensitive Information- this relates to any information about one's race or ethnicity, political opinions and/or memberships, religious beliefs or affiliations, philosophical beliefs, memberships of a professional or trade association, sexual orientation, health records, tax file numbers and criminal records. This information could be in written, photographic or other forms.

APP- Australian Privacy Principles. Thirteen of these exist.

OAIC- Office of the Australian Information Commissioner

Details

The School's information gathering and dissemination practices are outlined below.

The School collects and holds information that includes (but is not limited to) personal information, health and other sensitive information, about:

- Students and parents/carers before, during and after the course of a student's enrolment at NCS;
- job applicants, staff members, volunteers, contractors and specialist service providers; and
- other people who come in contact with the school.

APP 3 stipulates that all information collected by the School must:

- reasonably be necessary for one or more of the School's activities;
- be collected from the person to whom the information relates or their legal guardian[1];
- in relation to sensitive information, only be collected with the consent of the individual.

Reasonably necessary school activities requiring personal and sensitive information include (but are not limited to):

- communicating with school families;
- carrying out day-to-day administration;
- looking after students' educational, social and medical wellbeing;
- carrying out school marketing and fundraising;
- allowing the School to discharge its duty of care.

In accordance with APP 6, personal information will not be sold or otherwise transferred to unaffiliated third parties without the approval of the user at the time of collection.

In accordance with APP 12, upon request, the School must provide an individual with access to, and copies of, their personal information, except where there are reasons to refuse access. In such instances, the School must:

- verify the identity of the person requesting;
- consider whether any court orders exist that limit the sharing of information;
- consider whether or not to grant access in the event that a parent/carer does not consent to their child receiving access;
- consider whether or not to grant access to a parent where a child, depending on age or capacity, does not consent to the sharing of their personal information;
- provide written notice of the reasons for refusal and the avenues available for a complaint to be lodged.

The School may refuse access where the request is deemed to:

- be a safety concern;
- unreasonably impact on the privacy of others;
- be frivolous or vexatious;
- be unlawful;
- be commercially sensitive;
- be related to legal proceedings or ongoing negotiations with the individual concerned.

Where access is requested, the School:

- may charge a reasonable administration fee to provide the information;
- must respond within a reasonable period of time following the request;
- must consider alternative forms of sharing information, where access to specific information has been denied.

[1] Nb: Where a student in Year 10-12 is enrolling at NCS. They are required to give consent for their legal guardians to provide personal information on their behalf.

Upon a user's request, the School will use reasonable efforts to functionally delete the user and his or her personal information; however, it may be impossible to delete a user's entry without some residual information because of backups and records of deletions. However, student records cannot be removed.

Access to systems (including on-site databases and cloud storage providers) containing personal information is restricted to NCS staff members. Staff are granted levels of access to data in accordance with their responsibilities. The NCS Staff and Volunteer Code of Conduct document binds all employees and volunteers to strict confidentiality regarding personal and sensitive information.

NCS reserves the right to change this policy at any time by notifying users of the existence of a new Privacy Policy statement.

Relevant Legislation

Commonwealth Privacy Act 1988

Commonwealth Privacy Amendment (Enhancing Privacy Protection) Bill 2012

Health Records and Information Privacy Act 2002 (NSW)

Related Documents

Dispute Resolution Policy

Staff Code of Conduct

Volunteers Code of Conduct

NCS Enrolment Policy & Procedures

Consent Forms

Policy & Procedures for Engaging Third Party Providers

Data Breach Recording Tool

Data Breach Prevention Checklist

Data Breach Risk Assessment Process

Procedures

Data Collection & Storage

Personal information is generally collected via paper and/or electronic forms, email, face-to-face meetings, interviews and telephone conversations.

The School collects and stores data in a secure database. Access to this database is restricted and only granted for the purpose of fulfilling approved activities as outline in the policy section of this document.

Personal information is usually supplied by a parent or carer. In some cases personal information may be provided to the School by a third part such as, but not limited to, a counsellor or psychologist. Such information must only be used in line with the purposes for collecting data outlined above.

Updating Information- from time to time, staff, parents and other school community members may need to update their personal information via the various avenues the School provides.

Contractors and Service Providers- where an individual, organisation or business is employed to carry out work, whether educational or not, the School is required to collect and store personal information including, but not limited to Working With Children Check (WWCC).

Cloud Service Providers- when engaging data storage services, it is understood that:

- Collected data remains the property of the School and may not be used for any purpose by the service provider other than the purpose of providing data storage for the School;
- ongoing access and system support is guaranteed;
- all records will be handled by the service provider in accordance with the relevant legislation outlined in this document;
- the cloud service provider will promptly notify the School of any data breach;
- the cloud service provider will allow the School to audit data and/or allow the School to withdraw, delete or destroy data at anytime.

Job Applicants- personal information is provided by job applicants in the process of submitting a job application. This information is used for the primary purpose of selecting and appointing a successful candidate. Records of non-successful candidates are also kept for future reference in case of further employment becoming available.

Employees- The Privacy Act 1998 does not apply to employees of private organisations where:

- employment records (whether past or present) are directly related to the employment relationship[2].

Sensitive employee information is restricted to the Principal and to those to whom such knowledge is deemed necessary for the purposes of carrying out their role within the School. The information is only accessible by the Senior Executive and Principal's EA.

[2] https://www.oaic.gov.au/individuals/faqs-for-individuals/workplace/

Access to employees' financial arrangements with the School are generally restricted to the Principal and Finance Department.

Data Access & Sharing

Data access for employees is provided for the purposes of making informed decisions on a day-to-day basis. Data relating to students is accessible to staff via SEQTA Teach. Parents/carers are able to access educational and pastoral care information related to their child through SEQTA Engage. Parents and carers may request transcripts of all information recorded/collected by the School. Sensitive information related to staff is restricted to the Senior Executive.

Disclosure of Personal Information

The School may disclose personal information held by the school regarding an individual to:

- another school;
- government department;
- Medicare;
- medical practitioner;
- service providers to the school;
- parents/carers of a student;
- anyone personally authorised by the parent/carer of a student;
- anyone to whom the School is required to disclose information by law (e.g. where a student has or is moving to another school and that school requests information).

Data Storage & Security Procedures

Protecting Sensitive Information- access to all data stored at school is restricted. Data is stored using the following software platforms:

- SEQTA
- Consent2Go
- SAS Database
- Financial Information
- Medical Information
- Staff Information

Data Management & Security

Annually, a Data Breach Prevention Checklist will be completed by members of the Senior Executive to ensure that protocols are in place to protect data privacy.

Annually, staff will be in-serviced regarding the protocols for ensuring data privacy.

Data Retention & Disposal

- Staff details and personal information will be kept for a minimum of 7 years after the staff member leaves the School.
- Students' documentation will be kept for 7 years after they have left the school. Contact details will be maintained as part of the NCS Alumni database.

Data Breach Procedures

Eligible Data Breaches- an eligible data breach occurs when information held by the School is exposed or subjected to unauthorised access, sharing and/or modification. The School is required by law to inform affected individuals and the OAIC unless:

- mitigating action took place before serious harm was done to any individual;
- access to the information is unlikely to result in serious harm to the affected individuals.

Affected individuals and the OAIC are to be informed where information shared could reasonably be seen to result in serious harm. This harm could be physical, psychological, emotional, economic, financial and/or reputational.

Data Breach Procedure & Response Plan

1. Utilise the Data Breach Recording Tool & Data Breach Risk Assessment Process.
2. Immediately notify Heads of Schools and/or Principal.
3. Convene a data breach response team or appoint a person to investigate, assess risk and formulate a response to the breach.
4. Prevent a recurrence of the breach.
5. Prepare a breach report statement.
6. Consider notifying relevant authorities:
    a. submit the report statement to the OAIC (if required);
    b. inform the School Board;
    c. contact police if there is evidence of criminal behaviour.
7. Contact all affected individuals.
8. Prepare a record and report of circumstances and actions taken.

Enquiries and Concerns

For further enquiries regarding this policy, please contact the School. Any concerns regarding Privacy Procedures in relation to personal information should be made in writing and directed to the Principal.