



School Data Security Policy

Purpose

The purpose of this policy is to describe Clairvaux MacKillop College's approach to managing the College's information technology (IT) environment.

This Statement sets out how Clairvaux MacKillop College will manage personal information which is provided to or collected by it.

This policy must be read in conjunction with: BCE School Data Security Policy, IT Acceptable Use policy; Risk Management policy and Code of Conduct.

Rationale

Clairvaux MacKillop College's IT environment is intrinsically vulnerable to unauthorised or inappropriate use, release, accidental or deliberate damage and loss. Improper use compromises the underlying data, the resultant information assembled, decision making and the reputation of Clairvaux MacKillop College.

BCE and Clairvaux MacKillop College are bound by the Australian Privacy Principles contained in the [Privacy Act 1988 \(Cth\)](#) and as such may, from time to time, review and update this Privacy Statement to take account of new laws and technology and to ensure it remains appropriate to the changing school environment.

Policy Statement

The security of Clairvaux MacKillop College's IT resources is the responsibility of all users, including staff, students, parents, guardians, volunteers and contractors. Information security is a governance process that seeks to minimise risks to the College's processes and users of Clairvaux MacKillop College IT resources.

Principles

Clairvaux MacKillop College promotes a secure IT environment by applying the following principles:

- Confidentiality: ensuring that information is accessible only to authorised users
- Integrity: safeguarding and securing information, data, records and critical applications
- Continuity: owners of critical processes have access to IT resources
- Risk-based: evaluating threats, protect IT resources, promote a security-positive culture and encourage use that is ethical, responsible and lawful
- Performance: providing timely and accurate information on information security performance to leadership and promote continuous improvement.

Statement

Clairvaux MacKillop College will collect, hold, use and disclose personal information, as set out in this Privacy Statement.

What kinds of personal information does Clairvaux MacKillop College collect and how does a school collect it?

The type of information schools collect and hold includes (but is not limited to) personal information, including health and other sensitive information, about:

- Students and parents and/or guardians (Parents) before, during and after the course of a student's enrolment at the school, including;
 - 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);
 - Results of assignments, tests and examinations;
 - 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 school events;
- Job applicants, staff members, volunteers 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 school events;
 - workplace surveillance information;
 - work emails and private emails (when using work email address) and Internet browsing history; and
- Other people who come into contact with the school, including name and contact details and any other information necessary for the particular contact with the school.

Personal information provided:

Clairvaux MacKillop 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 provide personal information.

Personal information provided by other people:

In some circumstances, a 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. If a student transfers to a new school, the new school may collect personal information about the student from the student's previous school to facilitate the transfer of the student.

The purposes for which and how Clairvaux MacKillop College uses the personal information you provide:

Clairvaux MacKillop College 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, or for which you have consented.

Students and Parents:

In relation to personal information of students and Parents, Clairvaux MacKillop College's primary purpose of collection is to enable the school to provide a quality Catholic education to the student, exercise its duty of care and perform necessary associated administrative activities, which will enable students to take part in all the activities of the school. This includes satisfying the needs of the Parents, the student and the school throughout the whole period the student is enrolled at the school.

The purposes for which Clairvaux MacKillop College use personal information of students and Parents include:

- to keep parents informed about matters related to their child's schooling through correspondence, newsletters and magazines;
- day to day administration, including seeking the payment of fees;
- looking after students' educational, social, spiritual and medical well-being;
- to satisfy the College's legal obligations and allow the school 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 obtained, the College may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

Job applicants, staff members and contractors:

In relation to the personal information of job applicants, staff members and contractors, the College's primary purpose of collection is to assess and (if successful) engage the applicant, staff member or contractor, as the case may be.

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

- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking funds and marketing for the school; and
- satisfying the College's legal obligations, for example, in relation to child protection legislation.

Volunteers:

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

Who might the College disclose personal information to and store information with?

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

- other schools and teachers at those schools, including a new school to which a student transfers to facilitate the transfer of the student, and schools within BCE where concurrent applications for enrolment are made to those schools;
- government departments (including for policy and funding purposes);
- the Brisbane Catholic Education Office, the school's Archdiocese and the parish, and other related church agencies/entities;
- medical practitioners;
- people providing educational, support and health services to the school including specialist, visiting teachers, sports coaches, volunteers and counsellors;
- providers of specialist advisory services and assistance to the school, including in the area of Human Resources, child protection and students with additional needs;
- 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);
- agencies and organisations to whom we are required to disclose personal information for education and research purposes;
- people and organisations providing administrative, technology and financial services to the school;
- recipients of school publications, such as newsletters and magazines;
- students' parents or guardians;
- anyone you authorise the school to disclose information to; and
- anyone to whom we are required to disclose information by law, including child protection laws.

Sending and storing information overseas:

The College may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, the College will not send personal information about an individual outside Australia without:

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

BCE schools use centralised information management and storage systems (Systems) provided by third party service providers. Personal information is stored with and accessible by the third party service providers for the purpose of providing services to the BCE administered schools in connection with the Systems.

Online or 'cloud' service providers:

The College may use other online or 'cloud' service providers to store personal information and to provide other services to the school 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 server which may be situated outside Australia.

An example of such a cloud service provider is Microsoft. Microsoft provides 'Office365' (O365) including email, file storage and processes limiting personal information for this purpose. School personnel, BCE and their service providers may have ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering O365 and ensuring its proper use.

How does the College treat sensitive information?

In referring to 'sensitive information', the College 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; 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 sensitive information is allowed by law.

Management and security of personal information

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

Access and correction of personal information

Under the *Privacy Act 1988* (Cth), an individual has the right to seek and obtain access to any personal information which the College holds about them and to advise BCE or the school of any perceived inaccuracy. There are some exceptions to this right set out in the Act.

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 update any personal information that BCE or a school holds about you or your child, please contact the school's principal in writing.

The school may require you to verify your identity and specify what information you require. The school 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 school 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 (unless, given the grounds for refusal, it would be unreasonable to provide reasons).

Parents can also log on to the Parent Portal and correct and update some of their or their child's personal information at any time.

Consent and rights of access to the personal information of students

Clairvaux MacKillop College respects every Parent's right to make decisions concerning their child's education. Generally, a school will refer any requests for consent and notices in relation to the personal information of a student to the student's Parents. A 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. Parents may seek access to personal information held by a school or BCE about them or their child by contacting the school's Principal. However, there will be occasions when access is denied. Such occasions would include where the 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.

A 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 this.

Data Breach

Should the College or any member of the staff or student knowingly or by accident disclose personal data to third parties, the College will follow the Data Breach procedure

Data Breach Procedure

Upon becoming aware of a data breach, if the breach is electronic, the Network Manager and Assistant Principal Administration is informed so that a recall of the email or change the post in Teams can be attempted as soon as practicable, this may involve liaising with BCE IT Services. Emails can be received under the following circumstances.

- The sender and the recipient are in the same email group AND the recipient has not opened the email. eg If an email is sent to someone within cvxmck.edu.au or bne.catholic.edu.au and they have not opened the email, it can be retrieved.
- If you the recipient is outside cvxmck.edu.au or bne.catholic.edu.au, OR if the recipient has opened the email it cannot be retrieved.

The Assistant Principal Administration will advise the Principal of a data breach, attempts and success to retrieve the email or post in Teams.

The Principal will advise the Senior Leader of the data breach and work in collaboration with BCE IT Services and BCE Legal Services as to mitigate the data breach.

If the email or Teams post is retrievable, the Principal or Assistant Principal Administration will contact the Parent / Legal Guardian to advise them of the data breach, steps taken to mitigate the breach and success. The Parent / Legal Guardian are advised of their right to submit a complaint.

If the email or Teams post is not retrievable, the Principal or Assistant Principal Administration will contact the Parent / Legal Guardian to advise them of the data breach, steps taken to mitigate the breach and success.

The Principal or Assistant Principal Administration will contact all recipients of the data breach via telephone. Advise them of the data breach, ask them to delete the email or post, delete the deleted email or post, and provide a statement that the data breach has been successfully deleted. The Parent / Legal Guardian and the recipients are advised of their right to submit a complaint.