



PRIVACY POLICY

POLICY DETAILS AND DOCUMENT MANAGEMENT

Author:

Business Manager (Privacy Officer)

Approved by:

School Board

Endorsed by:

School Principal K-12

Review Due:

September 2029

Published:

September 2026

Policy Level		Dissemination	For Application	For Information
Board	☒	Board	☒	☐
School	☐	Executive Staff	☐	☐
		Administrators	☐	☐
Access		All Staff	☒	☐
Open	☒	Students	☐	☐
Restricted	☐	Public (Website)	☒	☐

REVISION HISTORY

Published	Version	Approved By	File Name
September 2026	1.0	Board	Privacy Policy V1

GENEALOGY

This Policy replaces: Privacy Policy V1
This Policy was cancelled and superseded by:

CONTENTS

PURPOSE	4
SCOPE AND LEGAL FRAMEWORK	4
1. PERSONAL AND SENSITIVE INFORMATION	4
2. COLLECTION AND NOTIFICATION	4
3. USE AND DISCLOSURE	5
4. STUDENTS, PARENTS/GUARDIANS AND CONSENT.....	5
5. ANONYMITY AND PSEUDONYMITY.....	5
6. IMAGES, RECORDINGS, DIGITAL SYSTEMS AND EMERGING TECHNOLOGIES.....	5
7. THIRD-PARTY PROVIDERS AND OVERSEAS DISCLOSURE.....	5
8. SECURITY, RETENTION AND DATA BREACHES	6
9. ACCESS AND CORRECTION	6
10. PRIVACY ENQUIRIES AND COMPLAINTS.....	6
11. Automated decision-making.....	6
12. RESPONSIBILITIES.....	6
13. COMPLIANCE AND MONITORING.....	7
14. REFERENCES.....	7

PURPOSE

Emmanuel Christian Community School (ECCS) is committed to protecting personal information and handling it lawfully, fairly, securely and transparently. This policy explains how ECCS collects, holds, uses, discloses, accesses, corrects, protects and disposes of personal information.

SCOPE AND LEGAL FRAMEWORK

This policy applies to personal information handled by ECCS about students, parents and guardians, staff, volunteers, contractors, job applicants, alumni and other people who interact with the School.

ECCS manages personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Notifiable Data Breaches (NDB) scheme and other applicable Commonwealth and Western Australian laws.

The employee records exemption under the Privacy Act may apply to some records directly related to a current or former employment relationship. ECCS will nevertheless handle employee information confidentially and securely.

1. PERSONAL AND SENSITIVE INFORMATION

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. It may include names and contact details, dates of birth, family information, enrolment and academic records, financial information, photographs, video or audio recordings, digital identifiers and online activity.

Sensitive information receives additional protection and includes health and disability information, religious beliefs or affiliations, racial or ethnic origin, criminal record, genetic information and biometric information or templates. ECCS collects sensitive information only where reasonably necessary and with consent, unless collection is otherwise permitted or required by law.

2. COLLECTION AND NOTIFICATION

ECCS collects only personal information that is reasonably necessary for its functions and activities, including:

- student enrolment, education, assessment, wellbeing, pastoral care, safety and administration;
- communication with families and the wider school community;
- recruitment, employment, volunteering and contractor management;
- financial administration, insurance, fundraising and school operations; and
- meeting legal, regulatory, reporting and duty-of-care obligations.

Information is generally collected directly from the individual or a parent/guardian through forms, meetings, telephone, email and approved school systems. It may also be received from third parties such as previous schools, health professionals, government agencies, referees or authorised service providers.

At or before collection, or as soon as practicable afterwards, ECCS will provide appropriate privacy or collection information, including the purpose of collection, usual disclosures, consequences of not providing information, access and correction rights, complaint arrangements and any likely overseas disclosure.

Where unsolicited personal information is received and ECCS could not lawfully have collected it, ECCS will destroy or de-identify it where lawful and reasonable to do so.

3. USE AND DISCLOSURE

ECCS will use or disclose personal information for the purpose for which it was collected, for a related purpose that would reasonably be expected, with consent, or where authorised or required by law. Sensitive information will be used or disclosed only as permitted by law and with additional care.

Depending on the circumstances, ECCS may disclose information to government and regulatory bodies, other schools, health and allied professionals, insurers, professional advisers, contractors and approved service providers, or another person authorised by the individual or their parent/guardian.

Personal information may be used for school communications, marketing or fundraising only where lawful and appropriate. ECCS will provide an opt-out where required and will not sell personal information.

4. STUDENTS, PARENTS/GUARDIANS AND CONSENT

For younger students, privacy notices and requests for consent will ordinarily be directed to a parent or guardian. As a student matures, ECCS may recognise the student's capacity to exercise privacy choices or seek access to information, having regard to age, maturity, circumstances, legal obligations and the student's best interests.

Requests by a parent or guardian for student information will be assessed having regard to parental responsibility, any court orders or other legal restrictions, the safety and wellbeing of the student or others, ECCS's duty of care, and the privacy of other individuals. ECCS may require proof of identity and authority before releasing information.

5. ANONYMITY AND PSEUDONYMITY

Where lawful and practicable, individuals may make general enquiries anonymously or using a pseudonym. Identification will be required where it is reasonably necessary for enrolment, education, safety, employment, financial administration, legal compliance or another core school function.

6. IMAGES, RECORDINGS, DIGITAL SYSTEMS AND EMERGING TECHNOLOGIES

Photographs, video, audio recordings and other student media are managed in accordance with the Student Images, Media and Emerging Technologies Policy and related procedures.

Personal or sensitive information must only be stored, shared or processed through approved school systems and services. Staff must not enter identifiable personal or sensitive information into unapproved generative AI tools, personal cloud storage, personal accounts or other unapproved digital services.

7. THIRD-PARTY PROVIDERS AND OVERSEAS DISCLOSURE

ECCS may use approved third-party and cloud service providers to support teaching, administration, communications, security and other school functions. The School will take reasonable steps to assess privacy and security risks, limit access to what is necessary, and require appropriate contractual and security safeguards.

Where personal information is disclosed to an overseas recipient, ECCS will comply with APP 8 and take reasonable steps to ensure the recipient handles the information consistently with the APPs, unless an exception applies.

8. SECURITY, RETENTION AND DATA BREACHES

ECCS will take reasonable physical, technical and administrative steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. Safeguards include controlled access, secure physical storage, approved digital systems, authentication controls, secure disposal and staff awareness.

Personal information will be retained only for as long as required for the purpose for which it is held and to meet legal, regulatory and record-retention requirements. When no longer required, it will be securely destroyed or de-identified where lawful and appropriate.

Actual or suspected data breaches must be reported promptly to the Privacy Officer and Principal. ECCS will contain and assess the incident, take remedial action and determine whether it is an eligible data breach. Where the NDB scheme requires notification, ECCS will notify the Australian Information Commissioner and affected individuals as soon as practicable.

9. ACCESS AND CORRECTION

Individuals may request access to personal information ECCS holds about them and may ask for inaccurate, out-of-date, incomplete, irrelevant or misleading information to be corrected. Requests should be made to the Privacy Officer.

ECCS will respond within a reasonable period and may refuse or limit access, where permitted by law, including where access would unreasonably affect another person's privacy, create a serious safety risk, prejudice legal proceedings or breach another legal obligation. Where access or correction is refused, ECCS will explain the decision and available review or complaint options.

10. PRIVACY ENQUIRIES AND COMPLAINTS

Privacy enquiries, access or correction requests, and complaints should be directed to:

- Privacy Officer (Business Manager), Emmanuel Christian Community School
- Phone: 08 9342 7377
- Email: admin@eccs.wa.edu.au

ECCS will acknowledge and investigate privacy complaints and respond within a reasonable period. If a person is not satisfied with the School's response, they may submit a complaint using the Complaints Policy.

11. Automated decision-making

From 10 December 2026, additional APP transparency requirements apply where ECCS arranges for a computer program to use personal information to make, or substantially and directly contribute to, a decision that could reasonably be expected to significantly affect an individual's rights or interests. Where applicable, ECCS will identify in its published privacy information the kinds of personal information used and the kinds of decisions involved and will review relevant systems periodically for such use.

12. RESPONSIBILITIES

- a) **School Board:** approves this policy and oversees governance.
- b) **Principal:** ensures the policy is implemented across the School.
- c) **Privacy Officer:** coordinates privacy compliance, access/correction requests, complaints, provider reviews and data-breach assessment.
- d) **ICT Manager:** supports technical security, incident response and approved-system controls.
- e) **All staff, volunteers and contractors:** protect personal information, use approved systems and promptly report suspected privacy or security incidents.

13. COMPLIANCE AND MONITORING

The policy will be reviewed every three years, or earlier if legislation, technology or school practices change.

14. REFERENCES

Related ECCS documents:

- Student Images, Media and Emerging Technologies Policy;
- Social Media Procedure;
- Records Management requirements and schedules;
- Complaints and Disputes Policy;
- ICT / acceptable use and cyber-security procedures; and
- Data Breach Response Procedure.

Key legal references:

- Privacy Act 1988 (Cth);
- Australian Privacy Principles;
- Notifiable Data Breaches scheme; and
- Privacy and Other Legislation Amendment Act 2024 (Cth).