



STUDENT IMAGES, MEDIA AND EMERGING TECHNOLOGIES POLICY

POLICY DETAILS AND DOCUMENT MANAGEMENT

Author: Principal

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	V1	Board	Student Images, Media and Emerging Technologies Policy

GENEALOGY

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This Policy was cancelled and superseded by:

CONTENTS

PURPOSE	4
SCOPE	4
CHRISTIAN FOUNDATIONS	4
DEFINITIONS	4
POLICY STATEMENT	5
1. PRINCIPLES	5
1.1 PURPOSE	5
1.2 CONSENT AND STUDENT VOICE	5
1.3 CHILD SAFETY AND PRIVACY	5
2. PUBLICATION OF STUDENT IMAGES	5
2.1 RESTRICTED SCHOOL ENVIRONMENTS	5
2.2 PUBLIC WEBSITES AND SOCIAL MEDIA	6
3. SCHOOL SOCIAL MEDIA	6
4. ARTIFICIAL INTELLIGENCE AND SYNTHETIC MEDIA	6
5. EMERGING RECORDING TECHNOLOGIES	7
6. PHOTOGRAPHY AND RECORDING BY STAFF	7
7. PHOTOGRAPHY BY STUDENTS, PARENTS AND VISITORS	8
8. LIVE STREAMING AND EXTERNAL MEDIA	8
9. STORAGE, ACCESS AND RETENTION	8
10. MISUSE OF IMAGES OR MEDIA	8
11. RESPONSIBILITIES	9
11.1 PRINCIPAL	9
11.2 STAFF	9
11.3 STUDENTS	9
11.4 PARENTS AND CARERS	9
12. BREACHES	9
13. RELATED SCHOOL DOCUMENTS	10
14. RELATED LEGISLATION AND GUIDANCE	10

PURPOSE

Emmanuel Christian Community School (ECCS) recognises the value of photographs, video, audio and other media in celebrating student learning, communicating with families and promoting the life and mission of the School.

ECCS also recognises that digital technologies, social media and artificial intelligence have increased the potential for images, recordings and personal information to be copied, manipulated, distributed or misused.

This policy establishes principles for the safe, respectful and responsible collection, creation, use, storage and publication of student images and other media.

SCOPE

This policy applies to:

- all ECCS students;
- employees, volunteers and contractors;
- parents, carers and visitors while participating in School activities;
- photographs, video and audio recordings;
- School websites, publications and social media;
- live streaming and digital communication platforms;
- artificial intelligence and synthetic media;
- drones, smart glasses, biometric technologies and other emerging recording or imaging technologies;
- media created during School activities, whether on or off campus.

CHRISTIAN FOUNDATIONS

ECCS believes that every person is created in the image of God and is therefore entitled to dignity, respect and appropriate protection.

The School will seek to use images, media and technology in ways that:

- honour God and reflect Christian character;
- respect the dignity, privacy and wellbeing of every person;
- protect children and young people from foreseeable harm;
- demonstrate honesty and integrity;
- use technology wisely and responsibly.

DEFINITIONS

- Artificial intelligence (AI):** Technology capable of generating, analysing or manipulating text, images, video, audio or other information.
- Deepfake:** Artificially created or manipulated audio, image or video designed to realistically represent a person saying, doing or appearing in a way that did not occur.
- Identifiable image:** An image or recording in which a person can reasonably be identified either from the image itself or from accompanying information.
- Media:** Photographs, video, audio, digital images, live streams, publications and other recorded or generated content.
- Public platform:** A website, social media account or other services where material can be accessed by people outside the School community without specific School authorisation.
- Synthetic media:** Image, video, audio or other media wholly or partly generated or materially altered using artificial intelligence or similar technology.

POLICY STATEMENT

1. PRINCIPLES

1.1 PURPOSE

Images and media will only be collected, used or published where there is a legitimate educational, operational, pastoral, community or promotional purpose.

The School will consider whether identifiable images are necessary to achieve that purpose.

1.2 CONSENT AND STUDENT VOICE

Appropriate consent will be obtained for the publication and external use of identifiable student images.

Consent will be collected through enrolment processes and where required specific activity permissions or other School-approved processes.

Where appropriate to their age and maturity, the wishes of the student will also be respected. A student should not ordinarily be required to participate in a photograph or recording where they express reasonable discomfort about doing so.

Consent may be withdrawn. Withdrawal will apply to future use where reasonably practicable but may not enable the School to retrieve material that has previously been lawfully published or distributed.

Specific consent may be sought where an image or recording is proposed for significant external publication, media coverage or another use beyond the ordinary activities of the School.

1.3 CHILD SAFETY AND PRIVACY

The safety and wellbeing of students will take priority over promotional or communication benefits.

The School will exercise additional caution when an image or accompanying information could reveal:

- a student's full identity;
- location or regular movements;
- personal circumstances;
- disability, health or wellbeing information;
- family circumstances;
- participation in counselling, student services or other sensitive programs;
- information that could place the student at increased risk.

Images will not normally be taken in toilets, changing areas, medical treatment spaces, counselling settings or other locations where students have a heightened expectation of privacy.

2. PUBLICATION OF STUDENT IMAGES

ECCS will use a risk-based approach when deciding where student images should be published.

2.1 RESTRICTED SCHOOL ENVIRONMENTS

Images may be shared through appropriately secured School systems (TEAMS, OneDrive), parent communication platforms (Seesaw), learning management systems (SEQTA), newsletters or other restricted environments where this supports learning and School community activities.

2.2 PUBLIC WEBSITES AND SOCIAL MEDIA

Greater caution will apply to material published on publicly accessible websites and social media.

When publishing publicly, the School will wherever reasonably practicable:

- minimise unnecessary identifying information;
- avoid combining a student's full name with a clearly identifiable image;
- avoid publishing information that reveals a student's regular location or movements;
- avoid unnecessary location tagging;
- consider group, activity or less-identifiable images instead of close-up portraits;
- compress close-up student images to web-standard low resolution (maximum 72 DPI)
- avoid announcing precise future student locations where this could create a safety risk;
- consider whether the communication purpose could be achieved without publishing an identifiable student image.

An image will not be published merely because consent exists. Staff responsible for publication must also consider whether publication is appropriate and proportionate to the purpose.

3. SCHOOL SOCIAL MEDIA

Only authorised personnel may publish content through official ECCS social media accounts.

Official accounts must:

- represent the School's Christian ethos and values;
- comply with School privacy, child safety and communication requirements;
- use approved imagery;
- be appropriately moderated;
- minimise unnecessary personal information;
- be reviewed periodically to remove material that no longer needs to remain publicly available.

ECCS will not require a student under 16 years of age to establish or maintain a personal account on a social media platform subject to Australia's social media minimum age restrictions.

School learning and communication involving students will occur through School-approved educational and communication systems rather than students' personal social media accounts.

Staff must not use personal social media accounts or private social media messaging as an alternative to approved School communication channels when communicating individually with students.

4. ARTIFICIAL INTELLIGENCE AND SYNTHETIC MEDIA

Artificial intelligence creates new risks because photographs, video and voice recordings can be altered to realistically depict events that never occurred.

ECCS prohibits the use of images, video, audio or other personal information relating to students or staff to create harmful, deceptive or inappropriate synthetic media.

This includes:

- deepfakes;
- face swapping intended to deceive, ridicule or harm;
- AI-generated sexual or intimate imagery;
- so-called 'nudification';
- voice cloning or impersonation;

- fabricated recordings or statements;
- AI-generated bullying, harassment or humiliation;
- manipulation of images in a way that damages the dignity, safety or reputation of another person.

Identifiable images, video or voice recordings of ECCS students or staff must not be uploaded to generative AI systems for image, video or voice generation unless the use has been specifically authorised by the School and appropriate privacy and consent requirements have been addressed.

School-created AI imagery must not be presented in a way that could reasonably mislead viewers into believing that an artificial image depicts an actual ECCS student, employee or School event.

Where realistic synthetic media is used for legitimate School purposes, its artificial nature should be disclosed where necessary to prevent misunderstanding.

Nothing in this section prevents ordinary, authorised editing such as cropping, resizing, colour adjustment, accessibility modifications or other reasonable production work that does not materially misrepresent a person.

5. EMERGING RECORDING TECHNOLOGIES

Technologies capable of capturing or analysing student images, voice, location or biometric information require particular care.

The use at School of technologies such as:

- drones;
- smart glasses or wearable cameras;
- facial recognition;
- biometric identification;
- automated video analysis;
- AI-enabled surveillance;
- other emerging technologies involving personal information

must be authorised by the Principal before use where they involve students or School activities.

Any proposal involving significant biometric, surveillance or similar high-risk technology must be subject to an appropriate privacy, child safety and information-security assessment and may require School Board approval.

6. PHOTOGRAPHY AND RECORDING BY STAFF

Staff may take photographs or recordings where reasonably required for School purposes and consistent with this policy.

School-managed devices should be used where reasonably practicable.

Where personal devices are authorised or necessarily used for School-related photography or recording, staff must ensure that:

- material is transferred promptly to an appropriate School-managed system (TEAMS, OneDrive);
- material is not retained unnecessarily on the personal device;
- automatic personal cloud backups are avoided where reasonably practicable;
- the images are not used for personal purposes or published through personal accounts.

Images created by staff in the course of their duties are School records or resources and must be managed accordingly.

7. PHOTOGRAPHY BY STUDENTS, PARENTS AND VISITORS

Students, parents and visitors are expected to respect the privacy and dignity of others when taking photographs or recordings at School activities.

The School may restrict or prohibit photography or recording at particular events or in particular locations. Parents and visitors should:

- wherever possible focus photography on their own child or family member;
- respect requests not to photograph particular students;
- not publish identifiable images of other students without appropriate permission;
- comply with instructions provided by School staff regarding photography or recording.

Students must not photograph, film or record another student or staff member in circumstances where doing so is prohibited, intrusive, humiliating, unsafe or contrary to School expectations.

Covert recording of another person is not acceptable except where specifically authorised or otherwise permitted by law.

8. LIVE STREAMING AND EXTERNAL MEDIA

Live streaming involving identifiable students requires appropriate authorisation, consent and risk assessment.

Particular consideration must be given to:

- the audience;
- whether the stream is publicly accessible;
- student identification;
- safeguarding risks;
- recording and subsequent availability of the stream;
- the disclosure of student locations.

Requests from television, newspapers, external organisations or other media involving identifiable students must be authorised by the Principal or delegate and may require specific parent/carers consent.

9. STORAGE, ACCESS AND RETENTION

Student images and recordings collected by the School must be stored and managed appropriately.

Access should be limited to people who require the material for legitimate School purposes.

Images and recordings must not be retained indefinitely without reasonable purpose.

The School will take reasonable steps to protect media from unauthorised access, disclosure, alteration or loss and will manage relevant material in accordance with its privacy, records management and information-security requirements.

10. MISUSE OF IMAGES OR MEDIA

Any suspected misuse of student or staff images, including unauthorised social media accounts, cyberbullying, impersonation, manipulated images, deepfakes or intimate imagery, should be reported promptly to an appropriate member of staff.

ECCS will respond according to the nature and seriousness of the incident and may:

- take steps to preserve relevant evidence;
- seek removal of material from a platform or service;
- contact parents or carers;
- provide pastoral or wellbeing support;
- apply student behaviour or staff disciplinary processes;
- report material to the eSafety Commissioner;
- seek advice from relevant authorities;
- report matters to Police or child protection authorities where required or appropriate.

Intimate or sexualised imagery involving a child must not be unnecessarily downloaded, copied, forwarded or redistributed when reporting an incident.

11. RESPONSIBILITIES

11.1 PRINCIPAL

The Principal is responsible for:

- oversight of this policy;
- authorising higher-risk uses of images and emerging technologies;
- ensuring significant incidents are appropriately managed;
- ensuring relevant staff understand their responsibilities.

11.2 STAFF

Staff are responsible for:

- checking relevant permissions before publication;
- using images only for legitimate School purposes;
- exercising professional judgement about what should be made public;
- protecting School media from inappropriate access or use;
- reporting suspected misuse.

11.3 STUDENTS

Students are expected to:

- respect the dignity and privacy of others;
- obtain permission before photographing or recording others where appropriate;
- use School and personal technology responsibly;
- not create or distribute harmful or deceptive media;
- report serious misuse of images or recordings.

11.4 PARENTS AND CARERS

Parents and carers are expected to support the School's child safety and privacy expectations when photographing, recording or sharing material involving members of the School community.

12. BREACHES

Breaches of this policy may result in:

- removal of material;
- restriction of access to School technology;
- action under the Student Behaviour Management Policy;
- staff disciplinary action;
- exclusion of visitors from School activities;
- referral to external authorities where appropriate.

13. RELATED SCHOOL DOCUMENTS

This policy should be read in conjunction with the School's:

- Privacy Policy;
- Child Protection Policy;
- Student Behaviour Management Policy;
- Cyberspace Policy and User Agreement;
- ICT / Acceptable Use requirements;
- Artificial Intelligence Policy;
- Social Media Procedures;
- Staff Code of Conduct;
- Records Management requirements;
- Complaints and incident management procedures.

14. RELATED LEGISLATION AND GUIDANCE

This policy has regard to relevant requirements and guidance including:

- Privacy Act 1988 (Cth), where applicable;
- Australian Privacy Principles;
- Online Safety Act 2021 (Cth);
- Australian social media minimum age requirements;
- Australian Framework for Generative Artificial Intelligence in Schools;
- eSafety Commissioner guidance for schools, students and families;
- WA requirements relating to the registration of non-government schools;
- applicable child protection and safeguarding requirements.