

Catholic Ladies' College



Social Media (Student Use)

clc.vic.edu.au

19 Diamond St, Eltham
Victoria 3095, Australia
03 9439 4077

ABN 44 058 164 891

Under the Stewardship of
Mary Aikenhead Ministries



MARY
AIKENHEAD
MINISTRIES

LOVE HOPE COMPASSION JUSTICE



Catholic Ladies' College Ltd
(ACN 058 164 891) (ABN 44 058 164 891)

Social Media (Student Use)

Preamble

Catholic Ladies' College (the College) is a Mary Aikenhead Ministry in the tradition of the Sisters of Charity. We seek to develop in each member of our community a contemporary understanding and application of the charism of Mary Aikenhead, the spirituality of the Sisters of Charity, the mission and vision of Mary Aikenhead Ministries and their values of justice, love, compassion and hope.

In responding to this call Catholic Ladies' College is a Christ-centred community established to educate, in partnership with parents, women of faith, integrity, individuality and compassion, confident of their own worth as women and wholly involved in the transformation of society.

Context

The College recognises the importance of social media tools as a mechanism for both individuals and organisations to engage and share information.

Students at the College enjoy the opportunities and rewards that being a member of the College community brings. It is subsequently expected that students will uphold the ethos of the College within and outside of the College and in all social media interactions.

The *Online Safety Amendment (Social Media Minimum Age Bill 2024)* amends the *Online Safety Act 2021* and requires 'age-restricted social media platforms' to take reasonable steps to prevent Australians under 16 years from having accounts on their platforms. There are significant penalties imposed by the federal government for breaching the minimum age obligation. While the legislation places obligations on social media platforms rather than schools, students and families should be aware that many platforms will prohibit access for users under 16 years of age once age-assurance measures are implemented. Students and families are expected to comply with platform age requirements, including restrictions for users under 16 years where applicable.

The College may also use school-managed social media accounts for marketing, communication and promotional purposes. This may include sharing information about College programs, events, achievements and community activities. All such use is managed in accordance with the College's privacy, child safety and communications policies, including obtaining appropriate consent for the use of student images or information.

This policy is informed by and supports the *Victorian Child Safe Standards*, particularly *Standard 9 – Physical and online environments*, which requires schools to promote safety and wellbeing in online environments and to minimise the risk of harm to students through digital technologies and social media use.

This policy applies to student behaviour both within and outside school where such behaviour impacts the safety, wellbeing or reputation of members of the College community.

What is Social Media?

Social media refers to online tools which provide individual users and/or organisations with the ability to create and share content in online communities. Social media tools include, but are not limited to, the following (also refer **Definitions**, page 3):

- Social Networking Sites – such as Facebook, LinkedIn, Instagram, Snapchat, Pinterest, Tiktok
- Video/Photo Sharing Sites – such as YouTube, Flickr
- Micro-Blogging Sites – such as Twitter, Yammer, Tumblr
- Weblogs – corporate, personal or media blogs published through tools such as Wordpress
- Forums & Discussion Boards
- Geo-spatial Tagging – such as Foursquare

- Online Multiplayer Gaming Platforms – Roblox
- Instant Messaging – SMS, WeChat, WhatsApp, Facebook Messenger
- Vodcasting and Podcasting
- Any other websites or devices (including mobile phones) that enable individuals to publish or distribute their own views, blogs, comments, photos, videos etc.

Purpose

The purpose of this policy is to set standards of behaviour for the use of social media that are consistent with legislation and the broader values and expectations of the College community

Intended Audience

Catholic Ladies' College staff, parents and students.

Guiding Principles

It is our policy that any individual using social media, must:

- use social media in a positive, respectful, responsible, inclusive and non-discriminatory manner
- refrain from acting in such a way that brings the College into disrepute or in a way that harms members of the College community
- not insult or present offensive or inappropriate content
- not misrepresent the College or any member of the College community.
- not share images or videos of others without permission
- comply with all legal and child safety obligations.

Definitions

Artificial Intelligence (AI) - technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy

Discussion Board - is an online communication tool that lets students and teachers take part in discussion in a virtual environment. It creates a virtual community of enquiry, allowing peer-to-peer discussions at any time and wherever Internet access is available

Geo-spatial Tagging - refers to the attaching of geographic coordinate information to images, video, and other media recorded by smartphones or GPS-enabled electronic devices

Instant Messaging - computer-based human communication between two users (private messaging) or more (chat room or "group") in real-time, allowing immediate receipt of acknowledgment or reply. Note that text messaging ("texting") uses the cellular phone service, whereas instant messaging employs the Internet

Micro-Blogging – is a combination of instant messaging and content production. With a microblog, you share short messages with an online audience to improve engagement. Social channels like Twitter, Instagram, Facebook and Pinterest offer popular platforms for microblogging

Multiplayer Gaming - is a video game in which more than one person can play in the same game environment at the same time, either locally on the same computing system (couch co-op), on different computing systems via a local area network, or via a wide area network

Sexting - Sexting is the sending or posting of provocative or sexual photos, messages or videos online

Social media - refers to online tools which provide individual users and/or organisations with the ability to create and share content in online communities

Social Networking Site – is an online place where a user can create a profile and build a personal network that connects him/her to other users

Vodcasting and Podcasting - Vodcasts combine audio and video, providing a visual element alongside the audio. Podcasts are audio-only, similar to a radio show

Weblog - is a regularly updated web page, where each item is presented in reverse chronological order, with the latest at the top

Social Media Code of Conduct for Students

Students are expected to show respect to others, including members of the College community. Students are also expected to give due respect to the reputation and good name of the College. Should students be in the position of using social media, they must:

- respect the rights and confidentiality of others
- not impersonate or falsely represent another person
- not use anonymity or false identities to engage in harmful, deceptive or inappropriate behaviour
- not bully, intimidate, abuse, harass or threaten others
- not make defamatory comments
- not use offensive or threatening language or resort to personal abuse towards each other or members of the College community
- not post content that is hateful, threatening, pornographic or incites violence against others
- not harm the reputation and good standing of the College or those within its community
- not film, photograph or record members of the College community without express permission of the College or use film, photographs or recordings without express permission of the other parties
- not use artificial intelligence (AI) tools to create, edit or disseminate content that is misleading, harmful, defamatory, or inconsistent with this Code of Conduct.

A failure to abide by the above expectations may constitute bullying or be unlawful. Refer to our CLC Positive Relationships: Bullying Prevention and Intervention Policy for details, available at <https://clc.vic.edu.au/our-school/policies/>.

Privacy Risks and Preventative Strategies

New technologies change the way students share personal information. As a result, social media sites present new privacy risks. If a social media entity is compliant with the *Privacy Act 1988 (Cth)*, the way they collect and use user information must be compliant with their obligations under the *Australian Privacy Principles* (refer to *CLC Privacy Policy* available at <https://clc.vic.edu.au/our-school/policies/>). In Victoria, schools must also act consistently with the principles reflected in the *Privacy and Data Protection Act 2014 (Vic)* and the *Health Records Act 2001 (Vic)* in relation to children and young people.

In relation to social media use, the following privacy risks arise:

- users may not have control over who sees the personal information they share online
- social media sites permanently archive personal information, even after users deactivate their accounts
- users may have their online posts republished by other users, an act over which they often have little control
- users open themselves up to personal and professional reputational damage as a result of social media over-sharing
- users open themselves up to online identity theft which often leads to serious financial and reputational damage.

To protect their privacy online, students are advised to:

- personally adjust the privacy settings on their social media pages
- only add people that they know and trust as online friends and contacts
- protect their accounts with strong passwords and do not share their account details, including passwords, with anyone
- not access social media sites by clicking a link provided in an email or on another website
- disable 'geo-tagging' or location information sharing on social media accounts and mobile devices to prevent strangers from knowing their personal home or College locations
- avoid 'checking in' at personal locations, such as their home, the College, other people's homes or while on excursions
- limit the amount of personal information (e.g. date of birth, address, information about your daily routine, holiday plans etc.) they provide on social media sites to prevent identity crime.

The College reserves the right to monitor publicly available online content that references the College, where it is necessary to respond to student wellbeing, safety or reputational concerns, in accordance with applicable privacy laws.

The College strongly recommends that class and year-level group chats do not exist. These spaces often create unnecessary social pressure and can contribute to conflict between students.

Parents and carers should speak with their child about their involvement in any group chats, their online behaviour, and the impact digital communication can have on themselves and others. These conversations are an important part of helping young people navigate online spaces safely and respectfully. Where group chats exist, student behaviour within them remains subject to this policy and other College policies.

Identity Crime Risks and Preventative Strategies

Identity crime is another risk of social media use. Identity crime describes the criminal use of another person's identity to facilitate in the commission of a fraudulent act. Students bear the risk of identity crime when they share personal information on social networking sites. Online identity theft has become more prevalent over the years, particularly as more and more users create online accounts and publicly share personal information.

The consequences of identity theft can include:

- personal and professional reputational damage
- physical harm
- substantial financial loss (e.g. credit card fraud).

Students are advised to be cautious of the personal information that they share online. Extreme care should be taken when providing personal details such as date of birth, address, phone contacts or educational details. Under new legislation, the federal government will implement strict privacy protections and age assurance technology to protect young people under the age of 16 years.

Students should not wear their College uniform in photos or share images of other students in uniform when posting on Social Media.

Reputational Risks and Preventative Strategies

Whenever users communicate through social media, their comments and posts are viewable by a large audience. In this way, all online communications will reflect on the user and their reputation. While this digital representation may have negative repercussions on the student, the College may also be vicariously affected.

In order to avoid reputational damage, students are advised to:

- remove content that may negatively reflect on them or the College
- think before they post and reflect on the potential harm the post may pose
- gain permission from the College before publicly sharing College information
- adjust their online security profile to limit the people who can see their personal information.

Sexting

Sexting is the sending or posting of provocative or sexual photos, messages or videos online. Sexting is treated differently under federal and state or territory laws but in general, sexting will constitute criminal conduct when it involves students aged under 18 and when it involves harassment or bullying. In some circumstances, the creation, possession or distribution of such material involving minors may constitute a criminal offence under Australian law. Where sexting involves minors, the police must be notified.

Refer to the *CLC Cyber Safety and Harassment (Student Against Student)* policies available on CLC Connect.

Use of Social Media for Educational Purposes

The College may utilise social media platforms as part of its educational programs. Staff may use College-managed accounts (e.g. YouTube or similar platforms) to deliver, support or enhance learning activities.

Such use must comply with relevant College policies, including the *CLC ICT Policy*, *CLC Child Safety & Wellbeing Policy* and *CLC Staff Code of Conduct*, and must ensure appropriate supervision, privacy protection and safeguarding of students.

Implementation

All College staff are responsible for implementing the *CLC Social Media (Student Use) Policy* available at <https://clc.vic.edu.au/our-school/policies/>. This policy is implemented through:

- staff training
- student and parent/guardian education and information
- effective incident reporting procedures

- effective management of bullying incidents when reported
- effective record keeping procedures
- initiation of corrective actions where necessary, and
- allocation of the overall responsibility for the effective implementation of this policy to the Deputy Principal Student Wellbeing.

Breach of Policy

A breach of this policy may also involve a breach of other College policies, and this policy should be read in conjunction with:

- *CLC Cyber Safety policy*
- *CLC Information & Communication Technology (ICT) policy*
- *CLC Student Use of Mobile Phones policy, and*
- *CLC Student Bullying Prevention and Intervention policy.*

A breach of this policy will be considered by the Deputy Principal and will be dealt with on a case-by-case basis. All reports of cyber bullying, hacking and other technology misuses will be investigated fully and may result in a notification to Police where the College is obliged to do so.

Sanctions for students may include, but are not limited to, the loss of computer privileges, detention, suspension, or expulsion from the College. Students and parents/guardians must be aware that in certain circumstances where a crime has been committed, they may be subject to a criminal investigation by police over which the College will have no control.

Reporting Pathways

Students, parents/guardians and staff are encouraged to report concerns about inappropriate, harmful or unsafe online behaviour as soon as possible.

Reports may be made internally to the College in accordance with this policy and related wellbeing and child safety policies. In addition, serious online safety issues — including cyberbullying, image-based abuse, non-consensual sharing of intimate images and harmful content — may be reported directly to the Office of the e-Safety Commissioner using the online reporting tools available at <https://www.esafety.gov.au/>

The College will support students and families to access external reporting pathways where appropriate and will cooperate with the e-Safety Commissioner and Victoria Police where required by law.

Related policies and guidelines

CLC Student Bullying Prevention and Intervention Policy

CLC Cyber Safety Policy

CLC Information and Communication (ICT) Policy

CLC Privacy Policy

CLC Student Use of Mobile Phones Policy

CLC Child Safety & Wellbeing Policy

CLC Child Safety & Wellbeing Recordkeeping Policy

The Office of the Children's eSafety Commissioner <https://www.esafety.gov.au/>
Criminal Code Amendment (Deepfake Sexual Material) Act 2024

Australian Government Department of Infrastructure, Transport, Regional Development, Communications Sports and the Arts <https://www.infrastructure.gov.au/department/media/news/social-media-minimum-age-legislation-passed>

Victorian Child Safe Standards <https://www.vic.gov.au/about-child-safe-standards>

Review Schedule

This policy will be reviewed annually, or earlier if required due to legislative, regulatory or educational changes, including changes to Commonwealth or Victorian online safety, privacy or child protection laws

Stage	Date	Ratified	Ratified by
Initiated	May 2020	May 2020	
Review 1	September 2025	November 2025	Executive
Review 2	June 2026	June 2026	Executive