HILLCREST CHRISTIAN COLLEGE

College Handbook 2018

Section: B. Policies | Social Media - Community

Ref:	B243
Last Reviewed:	Sep-18
Review Cycle:	Annual
Review Date:	Sep-19
Page:	1 of 4

SOCIAL MEDIA

Usage by the College Community

PURPOSE

The purpose of this policy is to encourage acceptable and beneficial use of social media by members of the College community, students, and families. It is recognised that many people may use or interact with social media at work and in a personal context.

There is great potential for the use of social media in the College community in terms of educational outcomes and as a means of communication.

However, the College community also need to understand the expectations of the College when using social media in a professional and personal capacity as there are also community risks that must be appropriately managed.

The College is committed to effectively engaging in social media in a respectful, meaningful, responsive, and equitable manner. It is important that everyone protect their privacy and consider both the potential implications of their online interactions (personally and professionally) and all materials they post online.

This Social Media community policy has been developed as a practical guide to support the College community to understand and meet the behaviors and obligations set out within the existing policies outlined within the scope of this document. The policy will address standards of behavior in the context of social media tools, rather than detailed procedures. It is not designed to cover every conceivable situation; therefore, emphasis is placed on guiding principles of behavior that are applicable under existing critical policies.

SCOPE

All students, staff, parents or carers and legal guardians, both future, current and past members of the Community.

WHAT IS SOCIAL MEDIA?

Social media is any form of online or web-based publication, forum or presence that allows interactive communication, including, but not limited to, Facebook, LinkedIn, Instagram, snapchat, blogs, forums, discussion boards, chat rooms, Wikis, Twitter, Pinterest and YouTube.

POLICY OVERVIEW

Members of the community will:
- use social media in a respectful and responsible 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, present offensive or inappropriate content; and
- not misrepresent the College or any member of the College community.

SOCIAL MEDIA RISKS

The following are some of the major risks associated with the use of social media:
- reputational damage to organizations and people;
- disclosure of confidential information and breach of privacy laws;
- posting of offensive, bullying, harassing, and discriminatory material;
- misuse of intellectual property and breach of copyright laws; and
- breaching professional and community expectations and standards.

HILLCREST CHRISTIAN COLLEGE

College Handbook 2018

Section: B. Policies | Social Media - Community

Ref:	B243
Last Reviewed:	Sep-18
Review Cycle:	Annual
Review Date:	Sep-19
Page:	2 of 4

RATIONALE

The purpose of this Policy is to set standards of behavior for the use of social media that are consistent with the broader values and expectations of the College community.

GUIDING PRINCIPLES

Community members should build community by:

- respecting the right`s and confidentiality of others;
- parents/carers and guardians serving as a positive role model for students and other community members;
- upholding the values of the College by acting with honesty, integrity, courtesy and professionalism, and not being discriminatory, defamatory, harassing or encourage law-breaking;
- being, accurate and relevant to the media being used;
- use social media to praise or acknowledge other is in the community;
- use social media as a communication tool and to facilitate communication amongst the College community;
- protect private information and copyright, privacy and other applicable laws when interacting on social media;
- accepting that the use of social media is a personal responsibility regardless of whether it is on behalf of the College or individual usage.

Community members should not allow the use of social media to impact on community by:

- allowing their online behaviour to show anything but respect for the dignity of each person;
- impersonating or falsely representing another person;
- using avatars or other means of hiding or misrepresenting their identity;
- bullying, intimidating, abusing, harassing or threatening others;
- using offensive or threatening language or resort to personal abuse towards each other or members of the College community;
- being negative or defamatory, nor mention specific individuals in the Community if there is a concern or issue as this is not the appropriate forum;
- posting content that is hateful, threatening, pornographic or incites violence against others;
- harming the reputation and good standing of the College or those within its community;
- posting images of footage of members of the College community without express permission of the College or use film, photographs or recordings without express permission of the other parties;
- posting inappropriate material about themselves that impacts on the community;
- making inappropriate contact with members of the College community; and
- breaching privacy laws, policies and/or principles.

Privacy Risks and Preventative Strategies:
- The advent of new technologies changes the way everyone share personal information. As a result, social media sites present new privacy risks.

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; or
- users open themselves up to online identity theft that often leads to serious financial and reputational damage.

HILLCREST CHRISTIAN COLLEGE
College Handbook 2018

Section: B. Policies | Social Media - Community

Ref:	B243
Last Reviewed:	Sep-18
Review Cycle:	Annual
Review Date:	Sep-19
Page:	3 of 4

In order to protect their privacy online, users 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;
- 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, the College or workplace locations;
- avoid 'checking in' at personal locations, such as their home, the College, work, other people's home or while on excursions; and
- 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.

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.

Everyone bears 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; or
- substantial financial loss (e.g. credit card fraud).

Reputational Risks and Preventative Strategies

Members of the College Community 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, educational details etc.

When in doubt, staff and students are advised to use the most secure privacy setting on their social media pages.

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 staff member or student, the College may also be vicariously affected.

In order to avoid reputational damage, Community members 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; and
- 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. The creation and/or distribution of the images may constitute child pornography. Where sexting involves minors, the police should be notified.

HILLCREST CHRISTIAN COLLEGE
College Handbook 2018

Section: B. Policies | Social Media - Community

Ref:	B243
Last Reviewed:	Sep-18
Review Cycle:	Annual
Review Date:	Sep-19
Page:	4 of 4

BREACH OF POLICY

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

- Cyber Safety Policy;
- Information & Communication Technology (ICT) Policy;
- Student Use of Mobile Phones Policy; and
- Other clients: Bullying Prevention & Intervention Policy.

A breach of this policy will result in the College having to take action. All breaches will be considered by the College 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.

Where a staff member breaches this policy, the College will take disciplinary action, including in the case of serious breaches, summary dismissal.

Where a parent/carer breaches this policy the College will act, including in the case of serious breaches, withdrawal of students and family members from the social media sites and potentially form the community.

Students and parents 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.

The College reserves the right to amend this policy at any time as it responds to the ever-changing use and impact of social media.

Policy Owner/College Executive