



Heights College

Social Media Policy

Our Commitment

The ever changing and inherently public nature of online communication presents a range of challenges in safeguarding the Heights College community, its staff and most importantly, the safety and security of its students. The College recognises that staff members may use social media channels outside school hours in a private capacity, however, such use can still have a negative impact upon the College and the College wishes to ensure that staff members take great care to avoid this by acting in the College's best interests when on-line at all times either on College or private equipment.

Scope

The scope of this policy extends to the Heights College Board, employees, including full-time, part-time, permanent, fixed-term and casual employees, contractors, volunteers and people undertaking work experience or vocational placements.

Responsibilities

Staff members must not use the College computer systems to access social media channels, unless the access is for teaching, pastoral care or educational purposes and the staff member has permission from the College Headmaster.

Staff members may also be held accountable for any social media use both within and outside the College, on school owned or private equipment, where the College may be recognised and its name brought into disrepute.

Inappropriate use of social media against the employer or co-workers outside of work hours and/or inappropriate personal use of social media during work hours may result in staff being dismissed for serious misconduct.

There are risks associated with the use of social media. These include but are not limited to;

- Breaches of the Heights College Staff Code of Conduct and Technology User Policy
- Plagiarism or breach of copyright conditions when using or reproducing material
- Excessive work-time used browsing social media applications
- Social media put to an inappropriate use
- Staff comments inadvertently bringing the College's reputation into disrepute
- Staff outlining personal political views whilst using their school contact
- Staff, through the use of pseudonyms or 'avatars' representing themselves as someone else either within the school or outside of the school
- Staff making promises or statements regarding the College's operations which are misleading
- Staff disclosing personal information relating to staff, students or parents or official information which is confidential or 'commercial-in-confidence'

Staff

1. Should read, understand and comply with the Staff Contract, College Technology User Policy, Social Media Policy and Staff Code of Conduct
2. Should declare their purpose and their position as a representative of the school, using an official staff account. Depending on how close the relationship is to the topic being discussed the staff may wish to provide a graduated level of identification.
3. Should not comment in depth on the activities of another sub-school or division of the school apart from providing factual information that is on the public record, unless staff have authority to do so.
4. Must avoid any statement that might bring the school into disrepute.
5. Must not commit the school to any action or initiative without appropriate authority.
6. Must not disclose information unless authorised to do so or unless it is already in the public domain.
7. Should comply with laws covering libel, defamation, privacy and the protection of intellectual property.
8. Must ensure all activities are in line with all other relevant school policies.

9. Must be apolitical, impartial and professional and avoid any statements that might be interpreted as advocating government policies or criticising the policies of political parties or groups.
10. Must protect personal information entrusted to the school from distribution into the public domain.
11. Must have approval from the relevant line manager to use social media in an official capacity.
12. Should take note of any copyright/Creative Commons and Intellectual Property notices attached to content they wish to use/repurpose.
13. Staff should cite or otherwise acknowledge content sources when they are known.

Inappropriate Use of Social Media

Inappropriate use, read in conjunction with the College *Technology User Policy* should include, but would not be limited to:

- Conducting private business during working hours.
- Using discriminatory, defamatory, abusive or otherwise objectionable language in content.
- Accessing, downloading or transmitting any kind of sexually explicit material, violent images including graphic images of blood or gore (without medical purpose).
- Accessing, downloading or transmitting information on the use and construction of weapons, explosives and other tools of violence or terrorism.
- Accessing, downloading or transmitting any material deemed to be illegal under Queensland State or Australian Commonwealth law.
- Compromising the privacy of any person.
- Attempting to gain unauthorised access to the computing resources of other organisations.
- Disrupting the integrity of the school's data or information services.

Definitions

Social Media – the use of web-based and mobile technologies to turn communication into an interactive dialogue

Participation – everyone who is interested has the opportunity to contribute and provide feedback on an issue through social media. The line between media and audience is blurred.

Openness – the majority of social media services encourage feedback and contribution allowing users to vote, comment and share information.

Conversation – social media are seen as a conversation between two, three or more users whereas traditional media is generally a one-way broadcast

Community – people who share a common interest (eg school, sporting team etc) are able to communicate effectively and instantaneously as soon as something occurs

Connectedness – most kinds of social media allow for links to other websites, video material, resources and people, creating a web of connectivity between users and content

Excessive -

Forms of social media include but not limited to;

- Social networking sites – eg Facebook, MySpace, Google+, Foursquare, LinkedIn, Bebo, Instagram etc
- Video and photo sharing websites – eg Flickr, YouTube, Wessabe
- Micro-blogging sites – eg Twitter, Posterous, Dailybooth
- Blogs – including corporate blogs, personal blogs or blogs hosted by traditional media publications
- Podcasts – including corporate podcasts and personal podcasts
- Forums and Discussion Boards – eg local discussion boards, Whirlpool, Yahoo! Groups or Google Groups
- Virtual game worlds – eg World of Warcraft, Fortnite
- Online encyclopaedias – eg Wikis such as Wikipedia, Geo-wiki, GeoNames, Sidewiki; and
- Any other websites that allow individual users or companies to use simple publishing tools

Relevant Legislation & Related Documents

This Policy is to be read in conjunction with the Heights College Statement of Faith as stated in the Heights College Constitution.

Heights College Code of Conduct

Heights College Complaints Policy and Procedures

Fair Work Act 2009

Privacy Act 1988

Privacy Amendment Act (Enhancing Privacy Protection) Act 2012

Child Protection Policy

Date approved	11 August 2020
Approval authority	Heights College Ltd Board of Directors
Date for next review	August 2021
Documents superseded by this Policy or Procedure	None
Distributed to	TASS Teacher Kiosk, Heights College Website

Revisions/Modifications			
Version	Date	Summary of changes	Reviewed by
1	October 2019	Creation of Social Media Policy	Business Manager
2	27 February 2020	Minor word changes throughout document. Distributed to Heights College Website added	Board Governance Sub-Committee
3	11 August 2020	Additional clause added under Relevant Legislation and Related Documents	College Board