**Australian Islamic College Perth Inc.**

**Social Media and Networking Policy and Procedures**

**Statement of Context**

The ever-changing and inherently public nature of online communication presents a range of challenges in safeguarding the Australian Islamic College community, its staff and most importantly, the safety and security of the AIC students.

The College recognises that staff members may use social media channels outside College 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.

This policy applies to all staff members employed by the College and all persons who work at or with the College in a casual or voluntary capacity.

**Policy**

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

Staff members may also be held accountable for any social media use both within and outside the College, on College 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 excessive personal use of social media during work hours may, in certain circumstances, result in staff being dismissed for serious misconduct.

**What are social media channels?**

There are various forms of social media channels and there are always new forms of social media being developed. Currently, the main forms of social media include, but are not limited to:

* Social networking sites: Facebook , MySpace, Google+, Foursquare, LinkedIn, Bebo and Friendster;
* Video and photo sharing websites: Content Communities such as Flickr, wessabe and YouTube;
* Micro-blogging sites: Twitter, Posterous, Dailybooth;
* Blogs: including corporate blogs and personal blogs or blogs hosted by traditional media publications;
* Podcasts: including corporate podcasts and personal podcasts;
* Forums and discussion boards: e.g. local discussion boards, Whirlpool, Yahoo! Groups or Google Groups;
* Virtual game worlds: e.g. World of Warcraft;
* Virtual Social Worlds: e.g. Second Life;
* Online encyclopaedias: e.g. Wikis such as Wikipedia, Geo-wiki, GeoNames and Sidewiki; and
* Any other websites that allow individual users or companies to use simple publishing tools, (together called Social Media).

These channels offer individuals the opportunity to connect with people, create and share information and ideas and develop relationships through online communities and networks.

**Procedures and Rules**

1. Staff members are required to declare their purpose and their position as a representative of the College when using an official staff account.
2. Staff members must not use social media channels, Skype or similar programs to communicate with current students unless for education or teaching purposes and the staff member has the permission of the Principal.
3. A personal relationship with current students via social media channels (for example, adding a current student as a ‘friend’ or ‘follower’ on Facebook , MySpace or Twitter or accepting an offer to join theirs) may exceed the accepted bounds of a teacher/student relationship and may leave the staff member open to allegations of improper conduct. Staff members must be aware of “Conditions of Use” for social media sites to be used for teaching purposes and that these conditions could preclude account use by students below certain ages (13 years is frequently stated).
4. Staff members are advised to use professional discretion before accepting ex-students or parents of current students as ‘friends’ or ‘followers’ on social media channels.
5. Staff members must not post images that include College staff or students on social media channels.
6. Staff members must not use the College's logo or create College branded accounts which could be interpreted as representing the College;
7. Staff members must not commit the College to any action or initiative without appropriate authority.
8. Consistent with privacy laws and other College policies, staff members must not, under any circumstances, reveal through social media channels confidential, proprietary or privileged information related to the College or its students, staff members, finance, policies or procedures, which is not otherwise publicly available.
9. Staff members should take note of and comply with any copyright/Creative Commons notices attached to content they wish to use/repurpose. Additionally staff must cite or otherwise acknowledge content sources when they are known.
10. Staff members 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.
11. Staff members must not either during or after hours, under any circumstances, disparage or speak adversely about the College or other Colleges, College business matters or activities, its staff or its students through social media channels.
12. Staff members are reminded that they should not have any expectation of privacy when it comes to content and information stored or posted in the social media environment. Even if staff members intend to keep the information private, it may unintentionally enter the public domain. For example, online content may inadvertently be viewed or accessed by colleagues, the media, students or families of students.
13. Staff members may not store or post inappropriate content and information in the social media environment, which is capable of being connected with the College, may adversely affect the College’s reputation, a student’s reputation and the individual staff member’s reputation.
14. Staff members may not identify or discuss co-workers or post photographs that include co-workers unless you have obtained their permission first.
15. Breach of this policy may result in disciplinary action being taken against the staff member. Disciplinary action may include limitation or removal of access to College Systems or termination of employment or a contractor’s engagement with the College.

The above requirements apply regardless of whether you have restricted the access to your personal site to selected persons only.

Implementation date: [11 September 2012]

Approved by: [Executive Principal]

Next review: [November 2013]