



One University. One World. Yours.

Policy Name:	Social Media - Protection of University Identity
Policy Number:	5-1004
Origin:	Web Steering Committee
Approved:	April 27, 2011
Issuing Authority:	Executive Management Group
Responsibility:	VP Administration
Effective Date:	May 1, 2011

1. Purpose:

To provide members of the University community with policy and procedures for the use of elements of Saint Mary's University identity, including the name "Saint Mary's University", its trade-marks, logos, brands and other signifiers that are used to distinguish the University.

In this Policy, the term "University Community" refers to faculty and staff of Saint Mary's University, as well as associated organizations such as those concerned with alumni affairs and student affairs.

This policy is developed and recommended by the Web Steering Committee of Saint Mary's University.

The Policy is administered by Public Affairs.

2. Definitions:

For the purpose of this policy:

- 2.1. The term **University Identifiers** refers to the name "Saint Mary's University", its trade-marks, logos, brands and other signifiers that are used to distinguish the University.
- 2.2. The term **associated organization** refers to one that wants to use elements of Saint Mary's University identity, including the name "Saint Mary's University", its trade-marks, logos, brands and other signifiers that are used to distinguish the University.
- 2.3. The term **official** refers to the University-sanctioned use of University Identifiers.
- 2.4. The term **account** refers to authentication credentials registered with any service or entity, including a social media site that permits the user to access the service. The account may be registered to an individual employee or a department. In order to obtain account for an online service, the user is required to disclose some information, such as name, email address, business affiliation, etc.

2.5. The term **social media** has the same meaning as in the Social Media and Personal Privacy Policy:

The term **social media** refers to a broad category of internet-based software tools, the primary purpose of which is the sharing of information and content. Social media (also known as social networking) consists of a growing body of technologies, software, tools, platforms and practices that enable people to shift between the role of audience and author for the purposes of communicating and networking via the internet, wireless networks or other electronic means in order to create, share, post or consume content, profiles, opinions, insights, experiences, perspectives, and other information and resources. These communications typically involve online groups or communities of users with shared or common interests who participate in electronic conversations or information sharing. Social media can take many different forms, including text, images, audio, video and other multimedia communications. More specifically, social media encompasses, but is not limited, to:

- social networking Web sites such as Facebook, MySpace, LinkedIn and Ning;
- forums, chat rooms and online message boards such as stock message boards, Yahoo! Groups and Google Groups;
- personal or company sponsored weblogs ("Blogs") such as Women on Their Way;
- micro-blogging services such as Twitter;
- photo and video-sharing Web sites such as PhotoBucket, Flickr and YouTube;
- podcasts such as iTunes and Zune;
- collaborative sites and wikis such as Wikipedia; and
- video blogs ("vlogs") such as those used by television stations and news outlets.

Social media allows people to connect in the online world to form relationships for a wide range of purposes. Members of the University community need to be mindful of their legal and other obligations when using social media. In particular, University personnel need to be aware that information posted to and shared through social media channels can pose significant business, legal and privacy risks and concerns for the university, its students and personnel.

Social media is inherently public and the University has an obligation to protect student privacy and to maintain the confidentiality of certain information.

3. Policy:

Protection of Saint Mary's University Identity:

Members of the University Community shall not use University Identifiers or other identifiers or communicate in such a way that would lead to the conclusion that the member is acting on behalf of the University except if they are authorized to do so. To do otherwise may be misleading and may damage the reputation of the University.

- 3.1. **University Graphic Standards:** All use of University Identity, online and offline, must conform to University Graphics Standards available from Public Affairs via SMUPort.
- 3.2. **Official Social Media Accounts:** All Saint Mary's University official accounts must be used for professional purposes only and only in a manner that reflects positively upon the University. No personal / home accounts can be used for conducting official university business, including the dissemination of information or

participating in social media activities. In addition, ITSS must be added as co-administrator for Pages, Groups, etc., in the event that the original administrator becomes unavailable or leaves the University. Contact Public Affairs to arrange for an ITSS co-administration.

- 3.2.1. **Approval to use Saint Mary's Name /Brand is required:** Creations of an official account requires official recognition and approval of the University. Approval can be requested from the Public Affairs Department at 420-5042.
 - 3.2.2. **Official Profiles:** Individuals authorized to create an official Saint Mary's University account, should consult SMUport for University Graphics Standards, including the use of the university logo and access to the photobank. Employee and department information, such as job title and business email address, must be included in the profile when an official account is created.
 - 3.2.3. **Security:** All Saint Mary's official account administrators will monitor postings and content on a regular basis. If there is more than one administrator, each administrator must have a separate / unique account for administration purposes only. This establishes clear responsibility for content and updates. Passwords should be kept in a secure place and changed at least once a year.
- 3.3. Members of the University community who communicate outside the University Community in a manner that may lead to the inference they are speaking or acting on behalf of the University but who have not been specifically authorized to do so, must take reasonable measures to clearly communicate that they are not acting in any official capacity. For example, University community members who participate in discussion groups that might lead to the inference that they are acting as a spokesperson for the University should take care to communicate that they are participating in their individual or professional capacity and not on behalf of the University.
- 3.4. If a member of the media contacts a member of the University Community (whether that person self identifies or the employee knows or has reason to believe that such person is a member of the media) and the member of the media is seeking comment from or input from the University, the member of the University Community shall refer such person to the University Public Affairs Department. If a faculty member is so contacted by the media and the media person is seeking any comment other than related to the faculty member's research or instructional expertise, the faculty member should refer such person to the University Public Affairs Department. To be clear, this policy is not intended in any way to preclude members of the University faculty from speaking to the media on any matter within their research or teaching expertise.

4. General:

General principles and policies of the University, such as those related to confidential information, personal information, and conduct apply to the use of University Identifiers.