University Policies and Procedures

10-01.06 – Social Media Policy

I. Policy Statement: The purpose of this policy is to provide rules of conduct for University departments and University employees when using digital and Social Media technologies to engage with others on behalf of the University. This policy does not apply to University faculty or staff members who use Social Media in a personal capacity, except to the extent that faculty or staff members acting in a personal capacity purport to represent the University. This policy is not intended to restrict communciations or actions required by state or federal law.

This policy also recognizes the importance of privacy in a student's personal activities involving the use of social media. It sets forth appropriate rules to protect student privacy interests while permitting the use of Social Media for academic and career-based activities.

II. Definitions:

A. In a Personal Capacity means acting as an individual, a person speaking for him/herself and not as a representative of the University.

B. Non-Public Access Information refers to the security information required to access a Social Media Account. Examples include but are not limited to passwords, log-in information and other private and confidential information required to gain access to a Social Media Account.

C. Personal Social Media Account refers to a Social Media account that allows social interaction and dissemination of information to others, created and maintained by a student, prospective student, employee or applicant for employment in whole or in part for private use. It does not include:
   1. an account on a Social Media platform owned or provided by an educational institution; or
   2. an account on a Social Media platform created by a student, prospective student, or applicant specifically for academic or University-assisted career-based activities.

D. Social Media are internet-based applications that enable users to participate in social networking by posting content and/or by exchanging content with other users. Examples of Social Media include but are not

limited to LinkedIn, Facebook, Twitter, YouTube, Flickr, Instagram, Tumblr, Vine, and Snapchat

E. University means Towson University.

F. University Site means a site with a "towson.edu" address.

G. University Social Media Account (USMA) is a Social Media account created by or on behalf of the University, and/or external sites that are linked to or embedded in a University Site and/or a Social Media account created by or on behalf of the University.

H. Using Social Media on behalf of the University or a department means acting as a spokesperson approved by the University for that purpose.

III. Responsible Executive and Office:

Responsible Executive: Vice President of University Marketing and Communications

Responsible Office: Department of Digital Strategy in the Division of University Marketing and Communications

IV. Entities Affected by this Policy: All members of the University community.

V. Procedures:

A. Use of Social Media by Faculty and/or Staff

1. Scope

Section V.A. of this policy covers activity on both USMAs, and on any other Social Media accounts where the user purports to speak on behalf of the University.

2. Responsibilities

The University expects all authorized participants in Social Media on behalf of the University to understand and to follow the procedures set forth in the Social Media Guidelines for Faculty and Staff (the "Guidelines"). The procedures set forth in the Guidelines may be amended from time to time without the need to amend this policy in accordance with Policy 06-10.00.

3. Sanctions

Failure to comply with any of the Best Practices and/or the Secure Practices set forth in the University's Social Media Guidelines for Faculty and Staff can result in loss of the privilege of linking a Social Media site to a University website, loss of allowed use of Towson logos, marks, or other website elements, (including the header and footer of the existing website, and/or loss of designation as a Social Media spokesperson for the University.

In addition, violating any other applicable University policies while using a Social Media site on behalf of the University may result in sanctions as set forth in the appropriate policy.

B. Student Social Media Privacy

1. Prohibited actions. University employees shall not:
   a. Require, request, suggest or cause a student, prospective student, or applicant to disclose, grant access to, or allow observation of Non-Public Access Information pertaining to the student, prospective student, or applicant's Social Media account.
   b. Require that a student, prospective student, or applicant change the privacy settings on a Personal Social Media Account.
   c. Require a student, prospective student, or applicant to designate a University employee or agent of the University as a "friend," a "follower," or any other designation that would afford the employee or agent access to a Personal Social Media Account.
   d. Require a student, prospective student, or applicant to log onto any Social Media account in the presence of a University employee or agent of the University.
   e. Require that a student, prospective student, or applicant provide names of the Social Media platforms that he/she uses.

2. Discipline. University employees shall not suspend, expel, discipline, penalize, or threaten to take any of the aforementioned actions against any student, prospective student, or applicant for refusing to provide information in response to a request that is prohibited under Section V.B.1. of this policy.

3. Limitations. This policy does not prohibit the following activities:
   a. University employees may require a student to provide access to a Social Media account provided that:
      i. the student has the option, at his or her own election, to complete the assignment or activity by using an existing Personal Social Media Account or by creating a generic Personal Social Media Account;
      ii. access is limited to the academic or career-based activity;
      iii. the student is not required to provide Non-Public Access Information; and
      iv. the academic or career-based activity is designed and administered in a manner that is consistent with the University's FERPA obligations.

   University employees are encouraged to obtain unit-level approval before instituting academic or career-based activities involving access to such accounts. In addition, University employees are encouraged to provide notice to students, in syllabi or other relevant written publications, when use of such accounts is required.

   b. University employees may access Personal Social Media Account information that has been voluntarily provided to them by a student, prospective student, applicant, or third party.

   c. University employees may access publicly accessible information relating to a student, prospective student, or applicant's Personal Social Media Account.

Related Policies: USM Policy V-1.20, Policy on Student Social Media Privacy

Approval Date: 09/21/2016

Effective Date: 09/21/2016

Approved by: President's Council 09/21/2016

Social Media Guidelines for Faculty and Staff

I. University Social Media Accounts

A. General

Social Media offers new ways for University employees to build relationships, and to take part in national and global conversations. The decision to use Social Media or to use and/or create a USMA is a business decision that must be made at the appropriate level for each department, considering its mission, objectives, capabilities and potential benefits.

If a department chooses to use a USMA, it should approve official participation and representation on specific Social Media sites. The University has an overriding interest and expectation in who may "speak" and what is "said" on behalf of the department and the University.

If the use of Social Media on behalf of the University is approved, a USMA is to be used for business purposes only. Electronic communications created, received, or stored on the University's electronic communications systems are subject to the University's Policy on Intellectual Property.

Any non-business use or intentional misuse of a USMA is a violation of this policy. Misuse of a USMA and prohibited activities include, but are not limited to:

1. sending and responding to private messages that are not related to University business or to a department's field of study;
2. engaging in vulgar or abusing language, personal attacks of any kind, or offensive terms targeting individuals or groups;
3. endorsement of commercial products, services, or entities;
4. endorsement of political parties, candidates, or groups;
5. lobbying; and
6. posting photos or videos that are not related to the mission of the University or to the department's field of study.

Anyone representing the University is responsible for the content they publish on Social Media sites.

B. Identification of Participant

During the use of a Social Media site on behalf of the University, the participant should identify himself/herself as follows:

1. Individual, from a University device conducting University business: The University employee should disclose his/her first and last name, contact information at work, and University department.
2. Individual, from a University employee clearly representing him/herself as a University employee but not conducting University business: The University employee should use a disclaimer such as "The postings on this site are my own and do not necessarily represent Towson University's positions or opinions."
3. Organizational, from a University or department controlled Social Media site: The department must disclose the name of the department and a single point of contact for inquiries or responses.

C. Creating a University Social Media Account

If you are an official representative of the University looking to get started in Social Media, University Marketing and Communications has everything you need to set up and maintain an account for your college, department or office. Simply follow the three steps below:

1. Notify your direct supervisor and, if necessary, obtain written approval from your department head, chair, dean or vice president.
2. Contact University Marketing and Communications so that your account can be listed in an accessible University Social Media directory. University Marketing and Communications can also help you set up your account, and support you with graphics, design, and branding for your Social Media presence.
3. Learn more about Social Media policies, best practices and guidelines, starting with those in this policy.

Also consult the "Guidelines for Responsible Computing" published by the Office of Technology Services:
http://www.towson.edu/technology/about/policies/computing.html

II. Best Practices and Guidelines

A. Be Yourself.

Transparency is a terrific asset in Social Media. If you are posting a message about the University or your department, it is important that you identify your affiliation with the University.

If you are posting to a personal blog, but are a University faculty or staff member, use a standard disclaimer, such as "The postings on this site are

my own and do not necessarily represent Towson University's positions or opinions."

A good resource on transparency in online communications is the Blog Council's "Disclosure Best Practices Toolkit" at http://www.socialmedia.org/disclosure/.

B. Respect and Comply with Terms of Use of All Sites You Visit

Do not expose yourself or the University to legal risk by accessing or using a website in violation of its terms of use. Review terms of use of all Social Media sites you visit to ensure your use complies with them. Pay particular attention to terms relating to:

1. prohibitions or restrictions on the use of the Social Media site, including prohibitions or restrictions on use for advertising, marketing and promotions, or other commercial purposes;
2. ownership of intellectual property used on, or information collected or generated through use of, the site;
3. requirements for licenses or other permissions allowing use by the site owner and other third parties of the University's trademarks or other intellectual property without appropriate University approval;
4. privacy rights and responsibilities of the site owner and users.

C. Be Responsible

The following is a checklist to ensure that your communications reflect the University's standards:

1. spell-check before posting;
2. provide appropriate context when linking to content, and remember that a link to another site (or sharing another person's message/post) could be construed as an endorsement;
3. keep conversations constructive and civil, and avoid the use of profanity, slurs or derogatory comments;
4. think twice before you post and remember that what you post has a long "shelf life" and a long reach. Archival systems save information, even if you delete a post. (If you are angry or passionate about a topic, you will want to give yourself some time to make sure that you are calm and clear-headed before posting.);
5. the use of hashtags is subject to the same guidelines as other communications. Double-check the spelling in your hashtag. Search for other possible current uses of the hashtag you are considering before posting. Check in with University Marketing and Communications if you are considering a hashtag to promote a University event or campaign to determine if (a) the hashtag is already going to be used by University Marketing and Communications to promote the event and/or campaign or (b) your

proposed hashtag may conflict with the University's approved messaging and branding for the event or campaign.

D. Be Accurate and Accountable

To increase your reputation for accuracy, it is better to first verify information with a source than to post a correction or retraction later. Make sure you have all the facts before you post, and cite and link to your sources whenever possible.

Of course, everyone makes mistakes. If you make an error, it is best to correct it quickly and visibly. Be the first to report your mistake, and your followers will appreciate your accountability.

E. Respect Copyrights and Intellectual Property

Always attribute proper credit for another person's work, and make sure you have the right to use something *before* you publish it.

Keep in mind that you must have permission to use the University's logos, graphics, design and/or branding *before* you use it.

F. Protect Confidential and Proprietary Information

It is easy to forget that online postings and conversations are not private. Always use good judgment and never post confidential or proprietary information about your department or division, the University, its students or alumni, or your fellow employees.

Remember to follow FERPA guidelines (University Policy on the Disclosure of Public Records), or http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)

Also see information on the Maryland Public Information Act at http://www.oag.state.md.us/Opengov/pia.htm

G. Respect University Time and Property

University computers and your work time are to be used for University-related business. It is appropriate to post at work if you have been instructed to do so or if your comments are directly related to accomplishing work goals, such as seeking sources for information or working with others to resolve a problem.

Please consult the detailed Acceptable Use Policy for more information.

H. Be Engaging and Share What You Know

Write in the first person and let your personality shine through. Ask yourself: what can I give my followers that they do not already have?

I. Stay Active, Timely and Relevant

If you stay active, topical and relevant, your audience will grow. The account should be accurate, and updated in a manner that reflects well on the University.

Embedding a widget on web pages is actively discouraged because of the risk that the Social Media account will not be updated frequently enough to be viewed as timely or relevant. University Marketing and Communications favors the use of calls to action to follow Social Media accounts in related content on published web pages. Invite website visitors to follow your Twitter account, but do not embed your Twitter feed on a website page.

J. Keep the University Connected

Notify your vice president or department head of the login and administrative credentials for an active Social Media account when it is first opened, and of any changes afterwards, in case it is necessary to access the account when you are not available (e.g., while you are on sabbatical).

K. Secure Practices

1. The information you post online could be used by those with malicious intent to conduct scams that steal confidential data. Be cautious in how much personal information you provide: remember that the more you post, the easier it may be for someone to use that information to steal confidential data.

2. Stealing passwords is a common way unauthorized users can gain access to Social Media accounts. When creating an account, follow password complexity best practices and choose password reset questions that cannot be easily guessed or answered through research.

3. Security technologies should be implemented to protect Social Media sites used by the University from unwanted user-generated content.