**ANR Social Media Best Practices**

Social media and social networking both refer to the interactions and communications of individuals in an online or virtual environment. Several types of social media have become a popular means of contacting friends, family members and even coworkers, such as Facebook, Twitter, LinkedIn, etc. These environments pose both a benefit and risk to the organization.

The California State Legislature has recently taken a strong stance on the use of social media in the workplace, which could change the way some of our staff and supervisors participate in social media. These best practices attempt to highlight the policy and give supervisors and staff a basis for communicating appropriately on social media sites. For specific questions, contact the Staff Personnel Unit at [anrstaffpersonnel@ucanr.edu](mailto:anrstaffpersonnel@ucanr.edu).

**Social Media:**

* is speech often protected by the First Amendment to the US Constitution
* is a form of communication most often covered under “protected concerted activities”, allowing employees to engage in criticism of his or her employer;
* policy prohibits unlawful conduct, but does not prohibit criticism of the employer;
* can unintentionally cause unlawful interference due to the possibility of union organizing activities, even for those non-represented employees;
* cannot be used as a means to create an impression of surveillance;
* cannot be used as a means to determine performance;
* cannot be used during recruitment activities or to supplement an interview;
* is often where confidential data is being shared;
* can unintentionally cause HIPPA violations;
* can reveal the employee’s religion, national origin, disability, or other protected class.

**Things to Consider**

Under a new California law, employers cannot request or require that **applicants or employees**:

* Disclose social media log-in credentials;
* Access personal social media in the employer’s presence; or
* Divulge any personal social media content. This is a broad requirement that also keeps an employer from requesting the personal social media content through “friends” of staff.
* The exception allows an employer (with the approval of HR-Labor Relations) to ask for access to personal social media content that may “be relevant to an investigation of allegations of employee misconduct or employee violation of UC policies, collective bargaining agreements and applicable laws and regulations."  This exception does not allow for broad or long term access.

**Best Practices for Supervisors**

* A supervisor may not ask, compel or require an employee to “add” a supervisor as a friend on social networking sites.
* An employee may “add” a supervisor for fear of reprisal, regardless of your intent. Consider their boundaries and how you would feel if a supervisor put you in the same position.
* Set boundaries on your own social media communications for work related purposes.
* Avoid the accidental impression of unlawful surveillance.
* Do not attempt to use social networking as a means to review staff comments, or feelings about work related issues in order to document performance, or gain access to confidential information.
* Be mindful of your interactions with your staff on social media.
* Do not require staff to utilize their personal social media sites to access or facilitate the use of work related sites. They may use a separate login with no personal information attached for work related social media sites.
* Ask yourself: is this employee’s activity on social media a protected activity?
* Ask yourself if you are treating all of your staff equitably as it relates to social media.
* Ask yourself if you are in compliance with the California policy on social media.

**Best Practices for Staff**

* Never feel pressured into giving access to personal social media sites to anyone. If access is required due to an investigation, HR will guide you through the process.
* Consider if requesting to add co-workers or supervisors to a personal social media site is going to cause a conflict of interest, or a blurring of the lines between your work and home life.
* Consider those co-workers who are also friends, and who they might give access to on their social media sites. Many sites allow friends of friends to see your pages.
* Do not fear reprisal for sharing valid, legal, opinions on social media sites.
* If you are responsible for running or participating in a work related social media site, you are not required to utilize any personal data. You can use a separate login specific to the work related site if you deem it necessary.
* If you do choose to participate in work related (vs. personal) social media sites avoid hateful speech, personal attacks, flaming, profanity, vulgarity, pornography, nudity and abusive language. These are prohibited by UC policy.
* Avoid using personal and confidential information on work related (vs. personal) social media sites.
* Be mindful of what you share; nearly everything on a social media site is public or can be discovered.