Municipal Technical Advisory Service
INSTITUTE for PUBLIC SERVICE

Published on *MTAS* (http://www.mtas.tennessee.edu) October 23, 2019

Employers & Social Media Passwords

Dear Reader:

The following document was created from the MTAS website (mtas.tennessee.edu). This website is maintained daily by MTAS staff and seeks to represent the most current information regarding issues relative to Tennessee municipal government.

We hope this information will be useful to you; reference to it will assist you with many of the questions that will arise in your tenure with municipal government. However, the *Tennessee Code Annotated* and other relevant laws or regulations should always be consulted before any action is taken based upon the contents of this document.

Please feel free to contact us if you have questions or comments regarding this information or any other MTAS website material.

Sincerely,

The University of Tennessee
Municipal Technical Advisory Service
1610 University Avenue
Knoxville, TN 37921-6741
865-974-0411 phone
865-974-0423 fax
www.mtas.tennessee.edu

Table of Contents

Employers & Social Media Passwords

Reference Number: MTAS-1393

A number of national trends related to the use of social media and employment practices have surfaced in recent years. Most notably, employers across the country have asked applicants to provide their social networking account information and passwords on job applications. Several states have made this practice illegal through legislation.

Tennessee joined the fray in 2014, passing legislation dealing with this ongoing issue in the form of the 'Employee Online Privacy Act of 2014 [1].' Effective January 1, 2015, the act prohibits employers from asking employees for their user names and passwords to social media sites and personal email accounts, as well as prohibiting the employer from compelling the employee to add the employer to their personal contact lists, or accessing personal internet accounts in the employer's presence.

Your city should be aware that improper use of social media information on applicants and employees may result in claims alleging discrimination, negligent hiring, violation of privacy, and open record conflicts.

In light of several federal laws including, but not limited to, GINA (Genetic Information Non-Discrimination Act) it is critical that employers not seek out information via social media that is not applicable to the essential functions of the job. In some cases, an employer simply viewing protected information about an applicant can have illegal implications.

If an employer elects to use social media profiles as part of the background check it is recommended that the employer get signed consent from the applicant that outlines exactly what information the city is looking for, and how it will be used in the hiring/employment process. In addition, employers should have a designated trained professional (one who is not involved in making hiring decisions) review this information, and should only pass on information to the hiring authority if it is essential to the job (i.e., poor communication skills, conflict in resume, etc.).

All other non-job-related information that is ascertained should not be shared with hiring authorities and must be redacted. This will help to ensure that personnel decisions are not based upon non-work related or discriminatory information such as disability status, genetic history, ethnicity, age, etc.

Here are a few guidelines:

- Employers should never ask for an applicant/employee's social media user name or password.
- Employers should never ask that applicants/employees log into their accounts during the interview process.
- Employers should avoid asking the applicants/employees if they use certain social media sites, unless the question is job related.
- Employers and hiring authority should not "friend" an applicant or an employee unless the accounts are both job related (i.e., city business) and of a non-personal nature.
- Employers should not create social media accounts for the purpose of searching for information that is not intended to be public or that is a violation of the social media site's terms and conditions.
- Employers should never try to bypass or manipulate a user's privacy settings for the purpose of gaining information and access to an applicant/employee's information.
- Employers should not use technology or third-party applications to draw out information from applicants/employees profiles for purposes of gaining access to the individual's information.
- If an employer elects to use social media searches as part of the hiring/employment process a policy stating exactly what information will be searched for and eventually used must be in place.

What is Fair Game?

- Employers may have a policy that restricts access to social media sites while on the job.
- Employers may have a policy that allows them to use public social media profiles in their applicant screening.

- Employers may follow their own policies and make employment decisions based on job-related discoveries on public social media sites.
- Employers have the right to prohibit use of city logos, uniforms, photos, etc. from employees' personal social media sites.
- Employers have the right to investigate claims of harassment or misuse of city property via social media.
- Employers have the right to prohibit behavior that is harmful to the city or its employees, and may interfere with the city's operation, the employee's job, or department's function.

Other Concerns

Workplace harassment can take place on or off the clock, and happens frequently via social media avenues. Employees should be aware that potentially harassing activity (on or off the clock) may be subject to open records laws and court subpoenas.

First Amendment Rights

Employers may not infringe on employees' or applicants' First Amendment rights. Employees may have the right to express personal opinions on their personal social media pages when off the clock, even if the employer doesn't agree with them. It is important to note that not all personal views on social media are protected from impact on an employee/applicant's job status.

In summation, employer policies should not be overly broad in that they prohibit activity allowed by federal laws such as the discussion of working conditions, wages, and other concerted activity. While the laws are still being deliberated on in many jurisdictions, most legal and human resource professionals agree: spying on applicants and employees sends a poor message that violating applicants'/employees' privacy is an acceptable business practice.

Links:

[1] http://www.capitol.tn.gov/Bills/108/Bill/SB1808.pdf