HUMAN RESOURCE ASSOCIATES

HR Consultants to Management

PERSONNEL NOTEBOOK

For Your Most Important Resource

SOCIAL NETWORKING

And The New Rules

The Internet

Since its introduction for commercial use in the early 1900s, the Internet, which in 1993 represented one percent of the world's two-way telecommunications, has expanded twenty years later to become the primary source of such communications at over 97 percent. Although the prevalent language use on the Internet has long been English at 27 percent, Chinese has now become the Internet's primary language at 29 percent.

Social Media

Social media (or social networking) is now used in even the most remote areas of the world. It has been deemed responsible for the creation of millions of new companies, the election of national leaders and the overthrow of governments.

Facebook, the real pioneer of social networking was launched by and for Harvard students in 2004 and opened for public use in 2006. It has within five years grown to one billion users world-wide. That's over 14 percent of the world's population now using just one of the many social websites available.

Social media was neither a new toy nor a passing fad to go the way of 3-D movies. This was different. Users were no longer restricted to the boundaries set by their software programs. They were no longer navigating on one-way streets along provided lanes controlled by program makers. This was the changing of the guard, the opening of the gates. This was User Generated Content (UGC). Instead of merely accessing provided information like news, television and film, social media users could create and publish their own content without the massive financial and technical resources formerly required. Their content could stand on its own without the usual layers of approvals and rejections.

Business

It didn't take long before this new blending of technology and social interaction came to the attention of entrepreneurs as well. Business and commerce are after all based on communication. The attraction of cheaper, faster, customized and personalized communication with customers and markets was about to create another explosion of the social media use and the internet. And in many cases the employees knew more about it than their employers. And

that's proved to be a good thing, for the most part.

Business discovered much to gain in the use and development of social media. Market research, communication with the public, sales promotions, discounts, the introduction of new products, the instant resolution of problems, newsletters without printing time and the development of personal relationships all at such a low cost. And with the new monitoring tools a company can quickly track the results of any promotion, ad, request or indeed any action. Also advantageous was the concept of employees being ever more involved and engaged in the personalization of the work they do. Another recognized value is the team building that develops as each employee identifies their specific areas of expertise and coordinates them with those of other employees.

Complications

Ownership: It didn't take long before the complications began. In a user generated media the individual who creates the content can, and often is considered to, be the owner of that content. So if an employee is using the internet and social media to create business opportunities for the company, does the employee own the content she created or does the company?

EdComm, Inc, a company in Pennsylvania, encouraged its employees to set up their profile using the company's template. Once an account was created, EdComm kept a copy of the account's password on file. When the company was later sold, many employees were terminated. The new owners changed the passwords and began 'mining' the accounts and business contacts. One employee, now shut out of her previous account, sued claiming ownership of the account as well as its contents. The company is still fighting the case in the courts, ownership is in question and the stakes are high for both profit and loss.

At this point the cause of the problem seems to be that the EdComm did not establish claim to ownership when they had the employee set up the account. A written policy and a signature acknowledgement by the employee could have avoided the difficult outcome; lesson learned. But this can also apply to patents. A policy or written agreement that re-enforces the understanding that all creations, inventions by the company on company time or on company facilities is owned by the company should be step one before the employee begins social networking.

Privacy: The acronym BYOD (bring your own device) is getting a lot of play these days. Because many employees, particularly salaried employees, perform some of their work during off-hours and off-site, some of that work is being done on their personally owned devices. That can create problems of ownership and privacy. So there will be a mixture business, social and personal information on one device and it's owned by the employee. Many companies do not allow employees to use their personal devices for company business at all. If you do require or allow them to do so, have them create separate folders for business and personal material and to clearly mark them as such. In addition, designate someone (or a team) to manage that separation and the appropriateness of the content. This means that MIS can access the employee's personal devices no matter where they are. Then if an employee leaves the company or loses the device, MIS can wipe all the business information from it while leaving the employee's private information untouched and intact.

Another issue of privacy arises when recruiting new employees. Employers sometimes require candidates to provide the password to their Facebook accounts. There certainly is a lot of information to be gleaned about the quality and history of an employment candidate there. That's true, but all too often this is information you shouldn't or don't want to, know. Information you wouldn't ask in an interview

may be information you don't want. Recent legal and EEOC cases have come about because a rejected employment applicant found that the interviewer accessed his Facebook account and discovered he was gay. In another case a rejected candidate claimed the reason for the rejection was that her Facebook account, accessed by the company, showed she had one child and was currently pregnant which she felt was the reason for her rejection. Currently three states now forbid employers to require candidates to provide their social media passwords or to require them to access their sites while in the company's presence.

This is a relatively new area for recruiters. The risk of privacy and discrimination issues are apparent as is the risk of making a bad hire. Although there are few good solutions yet, some companies are assigning non-hiring personnel or even non-employees to do the social networking research and deleting any potentially discriminatory information like race, religion etc. before it goes to HR or the hiring manager. In such cases the social search is documented as is the final reasons for the hire or the rejection.

Security: In a recent survey by MySammy and Holos Research, 77 percent of HR managers listed security as their primary reason for blocking employee access to social media. Their companies had a fear that proprietary, competitive and confidential information would be at risk. If the value of social media is desired, then monitoring tools, good management and solid policies are proving to be the best solutions.

Productivity: In that same survey, this was the second reason (67 percent) for denying access to social media, the fear that employees would waste time getting lost in the personal aspects of the social world. The answer from companies successfully using it, is to change managers from measuring employee in-put and begin measuring employee out-put. Managers can spend less time monitoring the busy-ness and energy being displayed and begin focusing on identifying the results expected and the quality and quantity delivered.

Harming Company Reputation: Coming in third place in the survey at 66 percent was the fear that a disgruntled employee would use social media to harm the company's reputation. The immediate answers all came down to creating good policy and orienting employees to what is acceptable and what is not. The initial policies provided by attorneys and HR consultants were adequate to the task. Policies that forbid lies, slanderous statements, threats, anonymous postings and the avoidance of creating a hostile work environment were reasonably effective until the newly re-formed National Relations Board (NLRB) imposed itself onto the issue.

The National Labor Relations Board (NLRB):

Most of us have lived our lives to this point without ever knowing or even hearing about the NLRB. Historically they were viewed as a federal governing group presiding over union disputes. With less than eight percent of the private industry work force being union there was little interest in their activities. However, the NLRB actually has jurisdiction over much more almost the entire work force whether union or not. And as we now learning, they have a great interest in expanding the role of unions across the nation and in all industry.

Unions today, like contemporary politicians, have learned the value of social media to spread their influence and message. And the NLRB openly intends to help them do that. In that endeavor they are charging companies, whose policies they see as too restrictive against union organizing activities, with labor violations.

For many companies so charged, there were many surprises in what the NLRB saw as violations. For example, policies that forbid employees to discuss wages or to publicly criticize the company they were being paid to represent were ruled to be unlawful.

Policies by COSTCO ruled in Violation:

"*Unauthorized posting, distribution, removal or alteration of any material on company property is prohibited*"

This was ruled in violation because it could be interpreted to mean that the employee would not be allowed to distribute union organizing materials.

"*Employees are prohibited from discussing private matters of members and other employees including topics such as, but not limited to, sick calls, leaves of absence, (Family and Medical Leave Act (FMLA), call outs, (Americans with Disabilities Act (ADA), accommodations, workers compensation injuries, health information etc."*

This was ruled in violation because an employee could interpret it to mean that he is not allowed to discuss working conditions or benefits.

"*Sensitive information such as membership, payroll, confidential financial information, credit card numbers, social security number, or personal health information may not be shared, transmitted or stored for personal or public use without prior management approval*."

"*Employees are prohibited from sharing "confidential" information such as employee's names, addresses, telephone numbers and email addresses*."

These were ruled in violation because contacting employees for union organizing purposes was necessary to accomplish that purpose as was the discussion of company benefits. The NLRB said that some of this information could become legal if it were accompanied by statements informing the employees of their union related rights and/or that nothing in this policy is intended to infringe upon those rights.

Even the "Employment at Will" policy had problems. The company's policy stated the basics regarding the employee's and the company's right to cease employment at any time and for any reason. It also stated that no employee had the authority to alter this Employment at Will policy. This was ruled in violation because it could lead employees to believe that no union contract would ever be allowed. The solution here is to identify someone who can alter the policy. So you can include a statement that says that only the owner (or CEO etc.) has the authority to alter this policy and that it must be must be in writing and signed by both parties.

Sao, can you prevent a disgruntled employee from disparaging your company or its employees? You can if you understand the concept of "concerted activity".

Concerted activity mans that as long as the employee is involved in legitimate union organizing-like activity such as complaining about wages, benefits and working conditions or trying to discuss joining or forming a union with other employees, he/she is engaged in concerted activity and that is protected activity. But common griping, personal attacks, lies, slander, threats, harassment etc. and actions not related to wages, benefits or working conditions is not concerted activity and is not protected.

One additional note, the NLRB rulings and all the protected activity regarding union organizing etc. only apply to non-exempt (hourly paid) employees. They do not apply to exempt (salaried) employees.

Bill Cook

Human Resource Associates

Have An Employment Question?

e-mail: wcook62@comcast.net