Churches should recognize, however, that numerous legal implications can arise from employee and employer use. Risks associated with employee use fall into two major categories: dissemination of disparaging and confidential information, and harassment and discrimination. Sadly, technologically savvy employees with the electronic world at their fingertips don’t always consider the legal, business and ministry implications of certain disclosures.

You’ve seen the headlines where employees have compromised their employer’s business reputations. Perhaps the most notable example is the Domino’s Pizza fiasco described above. However, many more examples abound. Several nurses at a Wisconsin Medical Center in 2009 posted pictures of patients’ X-rays showing the presence of an embarrassing foreign object in the patients’ bodies. The investigation was referred to the FBI due to federal laws including HIPPA and patients’ rights.

Confusion about what workers can or can’t post has led to a surge of more than 100 complaints at the National Labor Relations Board (NLRB), most within the past year, and has created uncertainty about how far social media policies can go. On August 18, 2011, the NLRB’s general counsel issued a lengthy report which was released to the public as Memorandum OM 11-74. The NLRB report outlines the facts of several interesting cases and concludes that federal law permits employees to talk with co-workers about their jobs and working conditions without reprisal, whether that conversation takes place around the water cooler or on Facebook or Twitter. These NLRB actions represent a new arena in which the agency is asserting itself in the private-sector workplace.

Employee use of social media can subject churches to liability for coworker harassment and discrimination. In the 2007 case of Derrick v. the City of Nashville, a female employee was able to show discrimination where her male manager made comments about women on a networking site: “What’s wrong with women these days?” and “Chicks seem to have more issues these days than Jet magazine and keep up more drama than daytime television and Jerry Springer combined.”

Employer use of social media can be just as problematic. Due to the rising popularity of social networking, many employers now include searches for information posted on sites as part of their regular background checks on job applicants. Most churches are looking for red flags—attitudes or behaviors that do not mesh with the core values and beliefs of the church. The challenge is that the profiles of applicants also include information about protected characteristics, such as race, age, disability, or genetic information. Even if the church chooses not to hire for legitimate reasons revealed by an electronic search, the mere fact that the employer was aware of the protected characteristics may be enough to cast doubt on the hiring decision. In addition, the search can foreclose...
an argument of ignorance of a protected characteristic, one of the most important defenses to discriminatory failure to hire claims. If a church is planning to use electronic screening, it should consider obtaining a candidate’s written acknowledgement that the church might search the Internet as part of its pre-employment investigation. To avoid a claim of disparate treatment, a church should screen all applicants if it screens any. If the search uncovers information that plays a part in the hiring decision, the church should keep copies to document the decision.

Also, churches may use social networking sites to monitor cyber-space behavior and activities of current employees. Employee use of social networking while on company time can hinder productivity. Thus churches can benefit from keeping a watchful eye, within reason. If a church manager adds an employee as a “friend” under false pretenses or by using a fake identity, the church could be susceptible to invasion of privacy claims. A church can avoid any appearance of coercion if it avoids managerial connections to employees on social networking sites.

Churches can reduce their risk of litigation and dissemination of confidential information by using a comprehensive policy governing social networking. Written policies should include a few basic provisions:
1. Social networking activities are subject to related church policies, e.g., computers;
2. There must be no impression—

                      “Employee use of social media can subject churches to liability for coworker harassment and discrimination claims.”

                      ……………………………………………………………

overt or implied—that the employee is speaking for the church;
3. The church has an interest in protecting its reputation and goodwill;
4. Employees must not use copyrighted church material;
                      “Most churches are looking for red flags, attitudes or behaviors that do not mesh with the core values and beliefs of the church.”

                      ……………………………………………………………

5. Employees must not disclose confidential information;
6. Employees must not disclose information about the church’s constituents;
7. Employees should expect compliance monitoring; and
8. The church may access information at any time without prior notice.

The best way for churches to guard against the numerous legal, business and ministry challenges posed by the use of social media is to develop and enforce a lawful and workable policy, nurture a positive environment, and educate their workforce. Churches should review their policies annually to keep them current with developing technology and related legal issues.

Cynthia Coffee is General Counsel at the Southeast Christian Church in Louisville, KY, an ECFA-accredited church.