

# Company Use of Social Media: Best Practices Checklist

## PLC Intellectual Property & Technology

A checklist of best practices for a company to consider when using social media in its business strategy.

### ESTABLISH CLEAR, WRITTEN TERMS OF USE AND PRIVACY POLICIES FOR ALL SOCIAL MEDIA SITES, SERVICES AND APPLICATIONS THE COMPANY OFFERS

- Establish a terms of use policy for online sites, services and applications to minimize undue business and legal risk.
- It should, for example:
  - require affirmative acceptance by third-party users (for example, by requiring users to actively click on an "I Agree" button) to increase the likelihood that a court will find the terms enforceable by the company;
  - include provisions that aim to protect the company from the misuse, infringement and misappropriation of its intellectual property assets and the unauthorized disclosure of its confidential and material non-public information; and
  - include provisions that aim to minimize liability for infringement of third-party intellectual property rights, defamation, privacy violations, employment-related harassment and the acts of third-party users, particularly for any content posted or uploaded by those users (referred to as user-generated content (UGC) (see also *Understand Legal Issues Associated with User-Generated Content and Take Steps to Minimize Risk*)).
- Establish an online privacy policy which is required by the law of some jurisdictions (including California) and is important to assist the company in complying with its privacy and nondisclosure obligations to third parties. The privacy policy typically addresses how the site collects, uses, discloses and maintains user data collected through the site.
- Ensure the terms of use and privacy policies cover any customized pages or channels offered by the company on

This is just one example of the many online resources Practical Law Company offers.



To access this resource and others, visit [www.practicallaw.com](http://www.practicallaw.com).

third-party social media sites (for example, the company's Facebook fan page or YouTube channels or communities).

For a model website terms of use and privacy policy, see *Standard Documents, Website Terms of Use* (<http://us.practicallaw.com/3-501-3816>) and *Website Privacy Policy* (<http://us.practicallaw.com/2-501-2704>).

### UNDERSTAND LEGAL ISSUES ASSOCIATED WITH USER-GENERATED CONTENT AND TAKE STEPS TO MINIMIZE RISK

Allowing users to post UGC on a website raises many legal issues for the site owner or operator, including exposure to liability for UGC that infringes third-party copyright and other intellectual property rights, violates an individual's publicity or privacy rights, is defamatory or obscene or is otherwise unlawful. Take appropriate steps to minimize risk for UGC, including, for example:

- Determine the applicability of safe harbor provisions under the:
  - Digital Millennium Copyright Act of 1998 (DMCA), which provides online "service providers" (as defined in the DMCA) with a safe harbor under certain circumstances for copyright infringement resulting from acts by their users (for example, an infringing video posted by a user on YouTube); and
  - Section 230 of the Communications Decency Act of 1996 (CDA) (giving computer services "providers" (as defined in the CDA) certain immunity for publishing tortious statements (such as defamatory statements) made by third parties.

- Implement procedures to take advantage of available safe harbor protections. For example, the DMCA safe harbor provisions require service providers to, among other things:
  - implement "notice and takedown" procedures for infringing content; and
  - designate an agent to receive takedown notices from copyright owners, notify the US Copyright Office of the agent's name and address and make this information available on the provider's website (for a model website DMCA policy, see *Standard Document, Website Copyright/DMCA Policy* (<http://us.practicallaw.com/7-502-3328>)).
- Implement comprehensive site terms of use (see *Establish Clear, Written Terms of Use and Privacy Policies for All Social Media Sites, Services and Applications the Company Offers*) that:
  - prohibit uploading of infringing, defamatory, obscene or otherwise unlawful or offensive content;
  - disclaim company liability for that content;
  - allow the site operator to remove content at its discretion; and
  - include procedures for filing and responding to third-party complaints as well as a clear DMCA-compliant "notice and takedown" policy.
- Ensure that the proposed use complies with all applicable laws (for example, traditional advertising laws) before making any further use of UGC (for example, using UGC for a promotion) and that necessary rights to use the UGC are obtained from all relevant third parties. For more information on advertising laws, see *Practice Notes, Advertising: Overview* (<http://us.practicallaw.com/2-501-2799>) and *Online Advertising and Marketing* (<http://us.practicallaw.com/4-500-4232>).

### REVIEW TERMS OF USE AND PRIVACY POLICIES OF THIRD-PARTY SOCIAL MEDIA SITES, SERVICES AND APPLICATIONS BEFORE USE

- Ensure that the company's use complies with each site's terms, which can vary significantly among sites and may include important restrictions. Pay particular attention to terms relating to:
  - 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 (for example, Facebook's Statement of Rights and Responsibilities (its terms of use) prohibit businesses from administering promotions through Facebook without Facebook's prior written consent);
  - legal responsibilities assumed with use of the site (for example, responsibility for complying with the "takedown" provisions of the DMCA);
  - ownership of intellectual property used on, or information collected or generated through use of, the site (for example, any of the company's copyrighted material and trademarks that might be posted on the site, or customer information the

company collects through the site) (for more information on intellectual property, see *Practice Note, Intellectual Property: Overview* (<http://us.practicallaw.com/8-383-4565>));

- requirements for licenses or other grants allowing use by the site owner and other third parties of the company's trademarks or other intellectual property; and
- recourse available to the company if its rights are violated (such as infringement of its copyrights) by other users.
- Ensure that the company's use complies with each site's privacy policies, which can also vary significantly among sites. Ensure that the site owner's privacy practices for any data disclosed by the company or collected by the company from users of the site are appropriate and sufficient for the company's intended use of the site.
- Monitor site terms and privacy policies regularly for updates and changes.

### ENSURE THE COMPANY'S USE OF SOCIAL MEDIA COMPLIES WITH ALL APPLICABLE LAWS

- Ensure legal compliance. Certain activities could expose the company to liability as well as serious reputational damage. The company should pay particular attention to the following laws:
  - defamation laws and prohibitions on unfair or deceptive acts such as false advertising. In particular, do not engage in or permit unethical marketing practices, including posting fake blogs, fake positive reviews, or fake negative reviews of competitors;
  - promotions, contests and sweepstakes law (for more information, see *Practice Note, Sales Promotions, Contests and Sweepstakes* (<http://us.practicallaw.com/1-500-4243>) and *Sales Promotions, Contests and Sweepstakes Checklist* (<http://us.practicallaw.com/2-500-9551>)); and
  - securities laws regarding market manipulation, insider trading, selective disclosure and disclosure of material non-public information (see *Publicly-traded Companies Should Take Care not to Violate Securities Laws When Using Social Media*).
- Ensure legal compliance with industry-specific rules as well.

For more information, see *Practice Notes, Online Advertising and Marketing* (<http://us.practicallaw.com/4-500-4232>) and *Legislation Governing Liability for Website Content Checklist* (<http://us.practicallaw.com/8-500-4353>).

### PROVIDE CLEAR GUIDANCE TO COMPANY MANAGEMENT ON COMPANY USE OF SOCIAL MEDIA, PREFERABLY IN THE FORM OF A COMPREHENSIVE POLICY

- Provide clear guidance that includes provisions to protect:
  - company intellectual property assets (such as trademarks, copyrights and patents);
  - the company's confidential and material non-public information;



- third-party confidentiality and privacy (including data protection with respect to personal information of employees, customers, suppliers and others); and
- the company's reputation and relationships with customers, vendors and other third parties (for example, statements made by employees may be imputed to the company, especially those made by senior management).
- Include in this guidance provisions to prevent:
  - discrimination;
  - harassment;
  - misrepresentation;
  - defamation; and
  - disparagement.
- Communicate this guidance clearly, monitor compliance and ensure enforcement is uniform throughout the organization (uneven enforcement can lead to discrimination claims).

For a model policy on company use of social media, see *Standard Document, Company Social Media Use Guidelines* (<http://us.practicallaw.com/9-501-1640>). For a model policy on employee use of social media, see *Standard Document, Social Media Policy* (<http://us.practicallaw.com/5-501-1524>).

### BE CAREFUL NOT TO IMPOSE UNNECESSARY OR IMPRACTICAL RESTRICTIONS ON COMPANY MANAGEMENT REGARDING USE OF SOCIAL MEDIA

Do not create too many restrictions on social media use to avoid unduly interfering with the company's appropriate, productive use of social media to advance business and legal objectives.

### CONSIDER USING SOCIAL MEDIA AS A LEGAL TOOL

- Consider using social media sites to prosecute, protect and enforce company intellectual property rights and defend against third-party infringement claims (for example, searching trademark uses and patent prior art, and monitoring against potential third-party infringement).
- Consider using social media as an effective way to share non-privileged information on legal topics, and obtain referrals to legal advisers and consultants.

### UNDERSTAND THAT USE OF SOCIAL MEDIA IS CHANGING HOW LITIGATION IS CONDUCTED

- Understand that litigators are using social media sites to:
  - make jurisdictional claims based on the worldwide accessibility of social media sites;
  - identify potential experts and other witnesses;
  - conduct discovery on adversaries and witnesses and obtain information that can discredit or impeach their testimony (for example, by requesting discovery of these parties' online profiles, postings, tweets, status updates or other

online communications, or otherwise issuing a subpoena to the relevant social media site for the information);

- A party conducting discovery of social media communications should narrowly tailor its discovery requests to relate specifically to its own defenses, the other party's claims and the other party's character and mental state. If a party is unable to obtain the requested discovery from the other party or the applicable social networking site company, it may still be able to obtain it where the online information is publicly available (for example, publicly available YouTube videos, tweets or Facebook profiles).
- Understand that postings made on social media sites might expose the company to potential liability and may be discoverable. The company may lose the protections of the attorney-client privilege or work product doctrine as a result of a disclosure of information through social media. For more information, see *Attorney-Client Privilege: Asserting and Waiving the Privilege Checklist* (<http://us.practicallaw.com/7-502-4771>). In-house counsel should warn companies about these risks, and include language addressing social media in document retention policies and litigation hold (<http://us.practicallaw.com/9-501-9293>) notices (see *Standard Document, Preservation Notice* (<http://us.practicallaw.com/0-501-1545>)).

### PUBLICLY-TRADED COMPANIES SHOULD TAKE CARE NOT TO VIOLATE SECURITIES LAWS WHEN USING SOCIAL MEDIA

Avoid the following traps when using social media sites to communicate with investors, market professionals and the public:

- Comply with Rule 10b-5 of the Securities Exchange Act of 1934 prohibits companies from making untrue statements or omitting material information. To prevent violation, monitor statements made by employees on social media sites to ensure they are not false or misleading, because they may be seen as manipulating the market and be attributed to the company. In addition, monitor links to third-party sites or content. Use of the links should be perceived as the company's endorsement of this information and the company could be held liable for any false or misleading statements by the third party.
- Monitor statements made by employees also to ensure employees are not tipping off investors by disclosing material non-public information in violation of insider trading laws.
- Comply with Regulation FD (17 C.F.R. 243.100 – 243.103) prohibits selective disclosure of material non-public information. Prohibit selective disclosures on social media in the same way as the company regulates disclosures in other media. Also, if desired, synchronize the release of any information on social media with more traditional news releases.
- Regulation G limits companies' use of non-GAAP financial information. Do not offer non-GAAP financial information without including comparable GAAP measures and a reconciliation of the information.
- Comply with securities laws that prohibit companies from soliciting stockholders for votes without first providing a proxy

statement, and from offering or selling securities to potential investors without first providing a prospectus (sometimes called gun-jumping). Ensure social media posts do not constitute unlawful solicitations or offers.

- Do not make "forward-looking statements" (that is, statements based on management's projections, estimates, expectations or assumptions) about the company or its performance, stock or prospects without also providing required cautionary language, written risk factors and disclaimers.

For more information regarding these risks, see *Practice Notes, Disclosing Nonpublic Information* (<http://us.practicallaw.com/2-382-5502>), *Complying with Regulation FD (Fair Disclosure)* (<http://us.practicallaw.com/1-383-2635>), *Registration Process: Publicity* (<http://us.practicallaw.com/1-381-0191>), *Using Non-GAAP Financial Information* (<http://us.practicallaw.com/8-502-4025>) and *Article, Guidance Policies on Future Operating Results* (<http://us.practicallaw.com/4-383-5034>).

### OBTAIN CONSENT BEFORE USE OF EMPLOYEES' OR THIRD PARTIES' NAMES, IMAGES OR INFORMATION THROUGH SOCIAL MEDIA FOR COMMERCIAL PURPOSES

- Use a comprehensive release document to explain to the employee or third party the purpose and extent to which the company will use his, her or its name, image or information, and memorialize consent.
- Avoid unauthorized use in order to reduce the risk of common law privacy claims such as:
  - public disclosure of private facts;
  - intrusion upon seclusion;
  - false light invasion of privacy; and
  - using the name or likeness of a person for commercial purposes.

### CONSIDER THE LEGAL RISKS ASSOCIATED WITH USE OF SOCIAL MEDIA TO RUN BACKGROUND CHECKS

- Avoid making employment decisions based in whole or in part on membership in a protected class (such as race, national origin, religion and sexual orientation) revealed through social media (see *Federal Employment Anti-Discrimination Laws Checklist* (<http://us.practicallaw.com/5-500-4793>)).
- Use the same protocols for social media screening of applicants or employees no matter their race, gender or other protected class status to avoid disparate treatment liability.
- Avoid discriminating against employees and applicants based on activity protected under the National Labor Relations Act (NLRA) revealed through social media.
- Comply with the Fair Credit Reporting Act (FCRA) and its state equivalent if applicable.
- Do not access password-protected electronic resources without proper authorization from the owner(s) to avoid liability under

laws governing electronic resources (such as the Stored Communications Act) and common law governing privacy.

- Ensure the company is in compliance with the "terms of use" policies of social media websites in any background check activities.
- Make employment decisions using vetted and accurate information, understanding that information posted on social media sites is often false or misleading, to avoid faulty hiring, terminations or promotions.

For a more complete description of these risks, see *Practice Note, Background Checks and References* (<http://us.practicallaw.com/6-500-3948>).

### AVOID TAKING RETALIATORY ADVERSE EMPLOYMENT ACTION FOLLOWING AN EMPLOYEE'S EXERCISE OF PROTECTED ACTIVITY THROUGH SOCIAL MEDIA

- Comply with federal and state laws that prohibit retaliation for the exercise of legally-protected rights.
- Employers considering terminations, demotions or other adverse employment actions should ensure that the reason underlying the decision is not a retaliatory response to an employee's exercise of certain rights, including:
  - whistleblowing;
  - unionizing;
  - participating in an internal investigation; and
  - taking a protected leave (including under the Family Medical Leave Act).

For more information about retaliation, see *Practice Note, Retaliation* (<http://us.practicallaw.com/5-501-1430>).

### BE CAREFUL NOT TO VIOLATE EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT IN THEIR USE OF SOCIAL MEDIA

- Do not restrict employee speech or take adverse employment actions that could violate the statute to the extent employees use social media to communicate about organizing, unions, or other rights and activities protected under the NLRA.
- Ensure NLRA compliance even in a non-unionized workplace (see *Ashley Furniture Industries, Inc. and Voces de la Frontera, NLRB Case 18-CA-18737*).

For more information, see *Practice Notes, Union Organization Process* (<http://us.practicallaw.com/5-501-0280>) and *Employee Rights and Unfair Labor Practices Under the National Labor Relations Act* (<http://us.practicallaw.com/1-502-5354>).

### DISCLOSE ALL MATERIAL CONNECTIONS WITH THIRD-PARTY BLOGGERS

- The Federal Trade Commission (FTC) requires advertisers to disclose connections with endorsers of their products if the



connection "might materially affect the weight or credibility of the endorsement." Material connections include, for example:

- payments to the endorser; and
- the provision of free products.
- If the company pays a blogger or provides free products to review, the company should:
  - advise the blogger of his obligation to disclose that he was given such consideration;
  - monitor the blogger's postings to ensure FTC compliance; and
  - monitor the blogger to ensure any claims made by the blogger about the company's products or services can be substantiated and are not deceptive or misleading.

For more information, see the *FTC's Guides Concerning the Use of Endorsements and Testimonials in Advertising*.

## REVIEW CORPORATE INSURANCE POLICIES TO ENSURE APPROPRIATE COVERAGE

- Understand that commercial general liability insurance policies may not cover liability arising out of certain online activities.
- Review existing insurance policies to ensure appropriate coverage and consider whether any additional insurance is desirable and appropriate. Additional insurance could include, for example:
  - cyber liability insurance that covers data breaches privacy and data security;
  - business interruption; and
  - media and web content liability.

## IN SUMMARY

Do:

- Establish clear, written terms of use and privacy policies for all social media sites, services and applications the company offers.
- Understand the legal issues associated with allowing users to post user-generated content and take steps to minimize risk related to that content.
- Review third-party social media sites', services' and applications' terms of use and privacy policies before using them.
- Ensure the company's use of social media complies with all applicable laws.
- Provide clear guidance to company management on company use of social media, preferably in the form of a comprehensive policy.
- Consider using social media as a legal tool.

- Understand that use of social media is changing the way litigation is conducted.
- Disclose all material connections with third-party bloggers.
- Review corporate insurance policies to ensure appropriate coverage.
- Do not:
  - Impose unnecessary or impractical restrictions on company management regarding use of social media.
  - Violate securities laws when using social media.
  - Use names, images or information of employees or third parties through social media for promotional or other commercial purposes without first obtaining such parties' consent.
  - Use social media to run background checks on applicants for employment and candidates for promotion without first considering the associated legal risks.
  - Take retaliatory adverse employment action following an employee's exercise of protected activity through social media.
  - Violate employee rights under the NLRA in their use of social media.

**Practical Law Company** provides practical legal know-how for law firms, law departments and law schools. Our online resources help lawyers practice efficiently, get up to speed quickly and spend more time on the work that matters most. This resource is just one example of the many resources Practical Law Company offers. Discover for yourself what the world's leading law firms and law departments use to enhance their practices.

To request a complimentary trial of Practical Law Company's online services, visit [www.practicallaw.com](http://www.practicallaw.com) or call **646.562.3405**.