

## Establishing Policies for Social Application Participation

Anthony Bradley, Nikos Drakos

Organizations should not shun Web participation for fear of bad behavior but should expect bad behavior as part of the social experience and should prepare carefully for it. Creating policies for social application participation is not a one-size-fits-all proposition. Policies will vary based on the goals of the particular social application and based on the characteristics of the participating community. To effectively formulate policies, organizations must understand the purpose of participation in a social application and the trust model of the target community.

### Key Findings

- Bad behaviors are a natural aspect of social application participation that should not be feared.
- Creating policies for social application participation is not a one-size-fits-all proposition.
- Each significant social application that is relevant to the enterprise requires distinct policy guidance.

### Recommendations

- Anticipate bad behavior as a natural aspect of social applications, and plan for the encouragement of desired behaviors and the discouragement of bad behaviors.
- Build a trust model for the purpose of community pairing to better understand and address the nature of desired community interactions, as well as the potential and risks of bad behavior.
- Formulate a multilevel approach to policies that address all significant social application participation coming from the enterprise.

## TABLE OF CONTENTS

---

Analysis .....	3
1.0 Establish a Community Trust Model.....	3
2.0 Approach to Policy Formulation .....	3
3.0 Three Levels of Monitoring Rules Enforcement .....	5
4.0 Impact on the Company Brand and Intellectual Capital .....	7
5.0 Recommendations.....	7
Recommended Reading.....	7

## LIST OF FIGURES

---

Figure 1. Policies, Procedures and Rules to Govern Corporate and Personal Use of Corporate Social Environments .....	4
--	---

## ANALYSIS

---

Do you belong to a social structure called a family? Do you consider it to be a positive social structure? Is the family's social structure devoid of bad behavior?

Most of us would answer "yes" to the first two questions and a resounding "no" to the third. Why? Because social structures, no matter how positive, always include some bad behavior. It is part of the human experience. Most of us would not avoid family involvement in anticipation of possible bad behavior. The same applies to community participation in social applications.

Organizations should not shun Web participation for fear of bad behavior but should expect it as part of the social experience and should carefully prepare for it. However, it's important to prepare carefully, because being too restrictive can have an adverse impact on participation and adoption, and being too liberal can have a negative impact on the effectiveness of community interactions and can degrade growth.

Creating policies for social application participation is not a one-size-fits-all proposition. Policies will vary based on the goals of a particular social application and the characteristics of the participating community. To effectively formulate policies, organizations must understand the purpose of participation in a social application and the trust model of the target community.

### 1.0 Establish a Community Trust Model

Not all communities are created equal; therefore, one policy will not adequately address all social application participation. For example, a financial services organization has a different approach to creating policies for establishing a social application directed at the general public than it would for a collaborative product and service design social application implemented for high-net-worth clients. The trust model for high-net-worth clients is very different from the trust model for the general public.

Although a broad Web participation policy is advisable, it is not the endpoint of the policy creation process but a foundation for more-specific policy formulation that addresses particular social applications. This is not to say that organizations must have a policy for each public Web-based social environment (Facebook, MySpace, Wikipedia and so on), but enterprises should have policies covering environments that are strategic to the company, whether public or private, on-premises or third-party hosted. The purpose of a trust model is to understand the characteristics of a particular community and its likely behaviors. This understanding illuminates the behavior opportunities and risks that influence participation in policy formulation.

Organizations should build a trust model for all significant and strategic participation in social applications. A trust model should capture information such as a basic definition of community and its characteristics, potential positive behaviors and their likelihood, potential bad behaviors and their likelihood, sensitivity to certain behaviors, required freedoms, a trust assessment, the potential for self governance and a framework for guiding rules and behaviors. Build the trust model with the goal of adding value to the subsequent effort of policy formulation.

### 2.0 Approach to Policy Formulation

Figure 1 contains a policy template to help IT leaders shape and govern participants' involvement in social applications.

**Figure 1. Policies, Procedures and Rules to Govern Corporate and Personal Use of Corporate Social Environments**

	<b>Corporate Social Environment (Internal and External)</b>	<b>Third-Party Public Social Environment</b>
<b>Corporate Use</b>	<ul style="list-style-type: none"> <li>■ General policy statement</li> <li>■ Purpose statement</li> <li>■ Specific policy statement</li> <li>■ Rules (minimal at start)                             <ol style="list-style-type: none"> <li>1. Human monitoring</li> <li>2. Automated enforcement</li> <li>3. Social monitoring</li> </ol> </li> </ul>	<ul style="list-style-type: none"> <li>■ General policy statement</li> <li>■ Purpose statement</li> <li>■ Specific policy statement</li> <li>■ Rules                             <ol style="list-style-type: none"> <li>1. Automated monitoring</li> <li>2. Human monitoring</li> </ol> </li> </ul>
<b>Personal Use</b>	Same as above, generally with more freedom	General policy statement (normally reflective of standing offline behavior policies)

Source: Gartner (June 2008)

Participants can be employees or external participants, such as customers and suppliers. The governance strategy depends more on the nature of the social application than on the participant group; however, enterprises must make allowances for participant groups that do not fall under the direct control of the enterprise that is stipulating the policy.

The figure is divided into four quadrants at the intersection of corporate use and personal use of an enterprise-operated social site and a public, third-party social site. Corporate use and personal use are independent of the participant group. For example, employee and customer groups can participate in a social site for corporate or personal use. The following sample social-site use cases should fall within one of the four quadrants:

- Customers participating in a corporate-run social site, for example, to rate product ideas in an environment for collaborative product design (upper-left quadrant)
- Employees participating in a corporate-run social site, for example, to share child care tips and arrange car pooling (lower-left quadrant)
- Employees participating in a third-party social site, such as Facebook, for corporate purposes such as keeping contact with geographically dispersed colleagues (top-right quadrant)
- Employees or the general public participating in a third-party, content-sharing site, such as YouTube, for personal reasons (lower-right quadrant)

The upper-left quadrant — reflecting corporate use of internally or externally facing corporate social environments — is understandably the most comprehensive in governance planning. Start by creating a general policy statement that applies to all social-site participation and reflects the basic expectations of online human behavior. This general statement often closely reflects corporate policy on social and ethical behaviors, and serves to remind people that guidelines for acceptable behaviors extend to online social interactions.

All corporate implementations of social software should have a well-defined purpose (see "How to Apply the PLANT SEEDS Framework for Enhanced Enterprise Web 2.0 Adoption"). Write a clearly articulated purpose statement that addresses why and how people are expected to

participate in a given social network (for example, to enable sales representatives to interact more tightly with channel partners to boost customer service). The purpose statement should not exceed one page. The purpose statement will go a long way toward discouraging inappropriate behaviors by explicitly stipulating expected, productive behaviors.

As an outgrowth of the purpose statement, develop a social-site-specific policy statement to address particular behaviors that are not covered in the general policy. Using the above example, the social-site-specific policy statement could state: "Here are the specific behaviors that we expect from our sales force when dealing with our channel partners."

Underneath the policy statement, establish rules to help moderate the social-software environment. These rules should be minimal at the start of your social application implementation to encourage participation and use. Focus on rules that address major risks, such as banning libelous language, profanity, sexually explicit comments and images, and harassing verbiage. A best practice is to take a "legal precedence" approach, where new policies and rules are added as participant behaviors dictate. This mitigates the risk of turning away participants because of overly restrictive policies and rules.

When exposing purpose and policy information to social-site participants, enterprises can be subtle by including the information as source documents in the environment, or they can be overt by requiring participants to indicate that they have read the documentation before joining the site. Participants may consider active indications to be intrusive, so enterprises must balance the potential annoyance level and possible negative ramifications against the need for participants to know that there are policy guidelines.

When formulating governance strategies for social sites, it's easy to focus on controls and restrictions and lose sight of the fundamental goal of building a thriving and self-sustaining community. Assess all governance policies, rules and mechanisms for their impact on the growth of community participation. Overly restrictive policies and controls can substantially inhibit community growth and can lead to the failure of the social application initiative. Managing an appropriate balance between freedom and control is crucial to community growth and maintenance, and must be tuned continuously.

### **3.0 Three Levels of Monitoring Rules Enforcement**

*The first level of enforcement is automated* (for example, immediate deletion of inappropriate images).

*The second level of enforcement is social monitoring.* This gives social-site participants the ability to identify content they believe to be inappropriate (for example, tagging a posting as an infringement of your company's intellectual-capital policy). Depending on participant item tagging or the use of social-monitoring functionality, such as "report abuse" buttons, you can trigger an automated rule to delete inappropriate content. Organizations can build a more robust social-content vetting capability into the social application, including functionality and a human social-monitoring structure.

*The third level of enforcement is human monitoring* (for example, a "neighborhood watch" assignment in which an employee housed in the IT organization or in the corporate business domain of the social-networking implementation patrols the social site to monitor social behaviors and review postings tagged as inappropriate). The human moderator can determine the appropriate response to the undesirable behavior (for example, taking action against the individual participant or instituting new policies or rules). Different social-site implementations require different levels of human involvement, depending on the nature of the information, how the bad behavior could manifest and the level of control the enterprise has over monitoring the

environment. For example, monitoring employee behaviors in an external site will reduce possible automated assistance because implementing governance tools in that environment is limited.

Don't be too strenuous when culling participant postings. Obviously, offensive postings can be deleted immediately; however, resist deleting postings merely because they reflect opinions that the enterprise may dislike. Trust is a critical component of a social site. If participants feel that the sponsoring organization is overcontrolling the community voice, then your company and the social environment will lose credibility and participation. Instead, comment on, tag or badge the posting to identify it as, for example, borderline inappropriate, a contrarian opinion, a competitor's viewpoint or counterproductive behavior.

*The upper-right quadrant in the attachment* — reflecting corporate use of a third-party public social environment — should encompass the first three governance actions discussed above, recognizing that enterprise control over the environment and automated enforcement are limited. The rules should include human and automated monitoring (for example, tell your employees that the company is monitoring behaviors in Facebook's corporate social circles). Appropriate responses will be limited to the institution of new policies and rules and to direct responses to individual participants, employees or external participants.

*The lower-left quadrant* — personal use of the corporate social environment — also can use the governance efforts of the upper-left quadrant, although your purpose statement can be less specific and can encourage more freedom. Such personal use might include building non-work-related interactions among employees geared to build tighter bonds to the company, such as friendship building, life experience sharing, book clubs, adventure clubs, personal time off exchanges, car pooling, child care or other social interactions that position the corporate environment as an extended support system for participants, including customers, employees and their families.

*The lower-right quadrant* — personal use of a third-party public social environment — understandably offers little opportunity for enterprises to proactively control behaviors. Therefore, this places your company in the role of monitoring after the fact and determining appropriate responses against the individual participants or the third-party sponsor. Monitoring and moderating this quadrant most often apply to employee behaviors; however, for some organizations, the general public is of great concern. Enterprises concerned with general-public misbehavior, such as copyright infringement and inappropriate brand use, must enact relevant policies.

For employees, create a general policy statement for expected online behavior. This statement, which often reflects standing corporate policies on appropriate and ethical behavior, underscores that company policy extends to online social interactions. Organizations should remind employees that inappropriate behavior in a real-world social setting (such as discussing unannounced products or financial information at a social event) is inappropriate online. Employees should understand that if their profile on public social-networking sites identifies them as an employee of your company, then their postings can have an impact on the company's reputation. A relevant example is corporate policy against public disparagement of your company, its products and services, and its clients and business partners.

According to Gartner research, approximately 15% to 20% of organizations ban (through URL filtering) access to social sites from the corporate network. Because many employees have personal-computing devices and Internet access, this measure does not obviate the need for corporate policies that address employee participation in external social sites.

## 4.0 Impact on the Company Brand and Intellectual Capital

Enterprises concerned about general-public misbehavior, such as copyright infringement and inappropriate brand use, must enact a second set of relevant policies. However, be careful not to tread on free speech and personal freedoms. If you do, then you risk alienating established and potential customers. Always assess the potential impact of policies and enforcement on your enterprise's Web reputation and brand recognition before taking action.

These policies require careful consideration and crafting, because they may need to stand up to legal proceedings. Ensure that policies and rules are vetted by your public relations, marketing and legal departments. Some industries, such as the motion-picture industry, have launched marketing campaigns around their anti-piracy and copyright infringement policies to extol the virtues of compliance and the industry ramifications of infringement in the hope of avoiding the need to take direct action against their customers.

## 5.0 Recommendations

We offer the following bottom-line recommendations for building an approach to social application participation policies:

- Don't preclude participation in social applications for fear of bad behavior.
- Anticipate bad behavior as a natural aspect of social applications, and plan for the facilitation of desired behavior and the discouragement of bad behavior.
- Build a trust model for the purpose of community pairing to better understand and address the nature of desired community interactions and the potential and risks of bad behavior.
- Formulate a multilevel approach to policy that addresses all significant social-application participation occurring from the enterprise.
- Understand the ramifications of policy rules and their enforcement on community adoption.
- Understand the impact of policy rules and their enforcement on your enterprise's Web reputation and brand recognition.

## RECOMMENDED READING

---

"Three Phases of Maturity Affect Social Software Deployments"

"How to Apply the PLANT SEEDS Framework for Enhanced Enterprise Web 2.0 Adoption"

"Five Major Challenges Organizations Face Regarding Social Software"

"Mitigate Risk But Don't Smother Wiki and Social Software Deployments"

"Answers to Client Questions on Social Software"

"Why Your Enterprise Needs a Corporate Blogging Policy"

## REGIONAL HEADQUARTERS

---

### **Corporate Headquarters**

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### **European Headquarters**

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### **Asia/Pacific Headquarters**

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### **Japan Headquarters**

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### **Latin America Headquarters**

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509