Social Media and Internet Communication Policy

There are many tools available today that enable people to publish and share content on the public Internet. These include social media sites such as Facebook, Twitter, Yelp, YouTube, and foursquare, subscription services such as Angie's List, as well as blogs, blog comments, forum posts, wikis, and other similar sites.

Whether you choose to participate in any of these forms of communication is entirely up to you. However, if you do participate in these activities, you must remember that you are a Company team member, and your postings can affect how the general public perceives the Company and its products and services.

The Company has the right to protect its business goodwill, and to make sure that nobody has made unauthorized uses or disclosures of its confidential business information. The Company must also ensure that anyone who uses social media or other public Internet tools maintains the Company's brand identity, integrity and reputation, while minimizing actual or potential legal risks, regardless of whether the origin of postings is inside or outside the workplace.

For this reason, the Company has enacted this Social Media and Internet Communication Policy. This Policy contains rules and guidelines concerning participation in social media and Internet communications that all team members—including executive officers, board members, and management—must follow at all times, *even on their own personal time*.

This Policy only applies to postings made on social media sites and other locations on the Internet that could potentially be viewed by members of the public. It does not cover private, non-public emails or other communications. However, all Company's team members must still comply with any other applicable the Company policies concerning appropriate email usage.

Usage Guidelines

The Company respects the right of its team members to use social media sites and other parts of the public Internet as a medium of self-expression, communication, and public conversation. The Company does not discriminate against employees who use these media for personal interests and affiliations or other lawful purposes.

The following guidelines apply to all use of social media or the public Internet by the Company team members, ***even when on their own personal time and on their own personal equipment***:

- Team members are free to identify themselves as a Company employee if they wish. However, team members who do so ***must*** state expressly that their views are their own, and do not reflect those of the Company or anyone doing business with the Company.
- If a team member is contacted by anyone about one of their posts, including a commenter or a member of the press, and is asked to discuss the Company business, the team member must speak with his or her manager before responding.

- Only team members who are specifically authorized by the Company are permitted to prepare and modify content for the Company's websites, any official Company blogs, and any of the Company's official social media presences. If a team member is uncertain about whether or not he or she is permitted to post certain content, he or she must discuss the proposed content with his or her manager prior to posting.
- If a team member sees a posting on the Internet from a customer or supplier of the Company that speaks adversely about any of the Company product or service, they *are not to respond directly to the poster*, but should instead forward the post to their manager.

Prohibitions

All Company team members are prohibited from doing any of the following things—***even on their own personal time and on their own personal equipment***—unless specifically instructed otherwise by an authorized member of the Company management:

- Speaking on behalf of the Company on the public Internet or in any social networking service
- Discussing or disclosing on the public Internet or in any social networking service any confidential information about the Company, including information about any Company client, vendor, product, trade secret, business plans, or financial information.
- Posting any content to social media sites or to the public Internet during working hours.
- Posting any content to social media sites or to the public Internet that contains a Company-owned trademark or logo or that contains any copyrighted Company content.
- Posting or "tagging" photographs or videos to social media sites or to the public Internet that depict any Company product or any Company facility or Company-sponsored event, or that depict any person engaged in the Company business.
- Posting any advertisement for a Company product or service to a social media site or to the public Internet.
- Using Company-owned equipment (including computers, mobile phones, at network connections) to conduct social networking activity.
- Posting a "deep link" to any Company-operated or affiliated website to the public internet or to any social media site. Team members may only post links to the public Internet front page of the Company or its brands (www.kay.com, www.jared.com, etc.)
- Posting any harassing, slanderous, abusive, or discriminatory content about any Company team member, client, or vendor.

Monitoring

Team members are cautioned that they should have ***no expectation of privacy while using the Internet, even on their own personal time, and even when using their own personal equipment.*** Team members' postings on social media and other Internet sites can be viewed by anyone, including the Company. ***The Company actively monitors the public Internet for***

comments, discussions, references, or other content that relates to the Company, its products, its team members, and the jewelry industry in general. Among the locations that the Company actively monitors are social media websites, tweets, blog comments, forum posts, and other public postings made by Company team members. The Company also uses tools to search and monitor these sites.

In addition, the Company actively monitors and, in many instances, saves and stores the activity that is conducted on its own computing, mobile computing, telephone, and networking equipment. This includes any data traffic passing through any Company router or server. Team members should have no expectation of privacy when using any Company-owned equipment or facilities. The Company may also use content management tools to monitor, review or block any content, including social media content, passing through its own equipment.

Team members should assume that the Company can see any communication, including social media and other public Internet postings, that are sent and received using the Company's own equipment.

Enforcement

The Company urges team members to report any violations or possible or perceived violations of this Policy to supervisors, managers or to Human Resources.

Any team member found to be violating this Policy is subject to immediate disciplinary action, including discharge. In addition, certain unauthorized disclosures to the public Internet can also be illegal, in addition to violations of this Policy. Examples of illegal behavior would include, but are not limited to, an unauthorized disclosure of the Company's confidential business information, or the use of the Internet to unlawfully harass others. Where necessary, the Company may, in addition to disciplining team members who violate this Policy, may also have to take appropriate legal action against the offending team member or others to protect its rights,

The following rules and guidelines apply to social networking and blogging when authorized by the employer and done on company time. The rules and guidelines apply to all employer-related blogs and social networking entries, including employer subsidiaries or affiliates.

Team Member Acknowledgment

I acknowledge that I have read this Policy, and that the Company has given me a copy of this Policy for my own records. I agree to comply with this Policy.

Signature: _____

Print name: _____

Date signed: _____