



Handcrafted Soap Makers Guild, Inc.

ORGANIZATIONAL POLICY

Privacy Policy

June 30, 2009

The privacy and security of information provided by members to the HSMG is of utmost importance. This policy clarifies what information the HSMG has and how it may be utilized.

All personal contact information supplied by current, past or potential members is considered confidential and may not be released or used for any purpose other than to contact the member and/or fulfill the HSMG's obligations to provide services to the member. Such services may include mail, email or phone contact, forwarding information to Stratus Insurance, etc. In no case may contact information be given to any person for any non-HSMG related activity.

Members may opt to include some or all of their contact information in an online Soapmaker or Vendor roster. The information so provided is public information (since it is displayed on the HSMG website) and may be given out to others if requested. However, no lists of Soapmakers or Vendors may be compiled and given or sold for non-HSMG activities (even through the names are publicly displayed).

Sensitive business or financial information may be collected when a member signs up. Such information is absolutely confidential and must be stored securely with limited access. Identifiable information may never be disclosed to anyone except the insurance company if requested. This information may be used to compile statistical analyses and reports, but never with the names of any individuals or any otherwise identifiable information published in any way. Anyone compiling such reports may, in the course of doing so, become aware of details about a specific person on business. The compiler must not write, note or copy the information or discuss any such details with any person for any reason.

Credit card information is collected in the HSMG shopping cart, and occasionally by phone or fax. All credit card information must be stored securely (encrypted, if stored on-line). Paper documents containing credit card information should be destroyed (shredded or burned) unless there is a legitimate need to keep the information.

In the course of performing duties for the HSMG, some individuals may have access to sensitive information. Therefore, any HSMG Board Member, sub-contractor, consultant or volunteer must comply with the following guidelines:

- No paper documents with sensitive information should be kept any longer than absolutely needed, and when kept, should be stored securely.
- All paper documents containing sensitive information should be shredded or burned (not tossed in the trash) once they are no longer needed.
- No credit card information should ever be sent by email, under any circumstances.
- When viewing sensitive information online, take reasonable precautions that your connection is secure. Use an appropriate firewall, especially when viewing documents through a public network (as in a hotel or library).
- Take reasonable precautions to protect any sensitive information on your personal computer, including password protecting access to the area, making your computer files inaccessible to others, etc.

- Delete any electronic files on your computer containing sensitive or personal information after you are finished with it and empty your recycle bin on a regular basis.

No private or sensitive information may be discussed with any other person for any reason.

Privacy Violations

In the event a Board Member, sub-contractor or volunteer discovers that any sensitive information in their control has fallen into unauthorized hands, the matter must be reported to the President immediately.

Any current, past or potential member who feels their privacy has been violated in some way by the HSMG should report the matter to the HSMG Ethics Committee.

Written by Marie Gale

Approved on June 30, 2009 by
the Board of Directors

History:

June 30, 2009 Original publication date