# **Social Media Policy**

## **Purpose**

The Company respects the desire of employees to use Social Media (see definition below) for personal expression. However, employees’ use of Social Media can pose risks to the Company’s and residents’ confidential, proprietary and sensitive information, can harm the Company’s reputation in the community, can expose the Company to discrimination and harassment claims, and can jeopardize the Company’s compliance with business rules and laws, including but not limited to the Company’s compliance with the Health Insurance Portability and Accountability Act (HIPAA) and related laws and regulations protecting residents’ protected health information (PHI).

To minimize these business and legal risks, to avoid loss of productivity and distraction from employees’ job performance, and to ensure that the Company’s IT resources and communications systems are used appropriately as explained below, the Company expects its employees to adhere to the following guidelines and rules regarding Social Media.

Definitions

Electronic Devices – Any device used for Electronic Communications or Electronic Information, including but not limited to: computers, laptops, tablets, digital cameras, video recorders, fax machines, copiers, scanners, telephone systems, smartphones, cell phones, and pagers.

Media – Any equipment on which Electronic Communications or Electronic Information is stored, including but not limited to: servers (including the cloud), CDs, DVDs, hard drives, flash drives, memory cards, and SIM cards.

Electronic Communications or Electronic Information – Including, but not limited to: electronic mail (email) messages, attachments, or links; instant messages; voicemail messages; text messages; digital photos; telephone conversations; Internet histories; social media posts, conversations, or messages; facsimiles; or any other kind of files, data, documents, communications, or messages, transmitted to, received by or printed from, or stored or recorded on any Electronic Device or on any Media.

Social Networking Communications – Any form of Electronic Communications or Electronic Information utilizing any form of networking environment, including but not limited to: all social networking forums or platforms such as Facebook, LinkedIn, Twitter, Instagram, Snapchat, YouTube, Pinterest, Tumblr, chat rooms, personal web sites, blogs and wikis.

Social Media – Including but not limited to all Social Networking Communications, Electronic Communications, and Electronic Information.

Protected Health Information – Including but not limited to any and all individually identifiable information about the physical or mental health condition or treatment of any individual, including but not limited to: any identifying information about a resident, such as the resident’s name or a photo or video of the resident; any information about a resident’s health condition or medication; and any information about payment for a specific resident’s care and services.

## **Standards for Compliance with Related Policies and Agreements**

All of the Company’s other policies that might apply to Social Media remain in full force and effect. Employees should always adhere to them with respect to all Social Media, whether or not you are using the Company’s IT resources and communication systems.

Social Media should never be used in a way that violates any of the Company’s policies or employee obligations. If your Social Media activity would violate any of the Company’s policies in another forum, it will also violate them in an online, electronic, or digital forum. For example, employees are prohibited from using Social Media to engage in activities that would:

* + Violate the Company’s policies on use of Electronic Devices or Media.
  + Violate the Company’s policies on confidential, proprietary and sensitive information.
  + Circumvent the Company’s ethics and standards of conduct policies.
  + Engage in unlawful harassment, discrimination or retaliation in violation of the Company’s policies or applicable law.
  + Violate the Company’s privacy or HIPAA policies or applicable law.
  + Violate any other laws or ethical standards (for example, using Social Media in a false or misleading way, such as by claiming to be someone other than yourself).

Employees who violate Company policies or applicable law while using Social Media may be subject to discipline, up to and including immediate termination of employment.

Protecting Residents’ PHI

Employees are absolutely prohibited from using Social Media in any way that would violate HIPAA or otherwise disclose or compromise residents’ PHI. This includes but is not limited to the following:

* DO NOT use Social Media to post, upload, send, or otherwise share or disclose a photo or video of any resident without prior written permission of the resident or the resident’s authorized agent as required by applicable law. You must use the Company’s authorization form to obtain such prior written permission. This prohibition includes photos and videos where the resident is not easily identifiable (e.g., a photo of the resident’s hand, a close up photo of any part of a resident’s body, or a photo of the back of a resident in the far background of the photo). It also includes photos or video where the resident is easily identifiable, whether in the photo or video itself or through a caption. This prohibition also includes photos and videos of residents participating in Company-sponsored activities or events. When in doubt, assume that you do not have permission to share a photo or video of the resident. Keep in mind that the resident or the resident’s authorized agency may revoke the permission at any time, which could require you to destroy all such photos or videos, including where posted.
* DO NOT use Social Media to post, upload, send, or otherwise share or disclose the name of any resident (even if just the first name or a nickname) without prior written permission of the resident or the resident’s authorized agent as required by applicable law. You must use the Company’s authorization form to obtain such prior written permission. When in doubt, assume that you do not have permission to share the resident’s name. Keep in mind that the resident or the resident’s authorized agency may revoke the permission at any time, which could require you to destroy all such photos or videos, including where posted.
* DO NOT use Social Media to post, upload, send, or otherwise share or disclose any information about a specific resident, even without a photo, video, or name, that could allow any individual to identify the resident without prior written permission of the resident or the resident’s authorized agent as required by applicable law. You must use the Company’s authorization form to obtain such prior written permission. This prohibition includes any resident’s age, biographical background information, unique medical condition, treatment or payment information, or other personal or identifiable information about a resident, whether alone or in concert with other information about the resident. This prohibition also includes any photos, videos, or other identifying information about the family members of any resident. When in doubt, assume you do not have permission to share any information about a specific resident. Keep in mind that the resident or the resident’s authorized agency may revoke the permission at any time, which could require you to destroy all such photos or videos, including where posted.

Use of Personal Electronic Devices during Working Time Prohibited

Employees are not permitted to use any personal Electronic Devices during working time. In addition, employees are not allowed to have or carry personal Electronic Devices on their person (e.g., in a pocket or a personal handbag) during working time when employees are in areas containing or otherwise have access to PHI or other confidential or sensitive resident information. For example, employees are prohibited from having or carrying personal cell phones, smartphones, or digital cameras when working with or near residents, resident charts or other medical documents, white boards containing resident information, or resident medications. If you have any questions about when you may have or carry a personal Electronic Device during working time, please contact Human Resources.

## **No Expectation of Privacy in Company’s IT Systems**

All contents of the Company’s IT resources and communications systems, including but not limited to all Company Electronic Devices, Media, and any other components of the Company’s computer, electronic, or digital system(s) or network(s) (collectively the “Company’s IT Systems”), are the property of the Company. Therefore, employees should have no expectation of privacy whatsoever in Electronic Communications or Electronic Information transmitted to, received by or printed from, or stored or recorded on the Company’s IT Systems.

You are expressly advised that in order to prevent misuse, the Company reserves the right to monitor, intercept, and review, without further or advance notice, every employee’s activities using the Company’s IT Systems, including but not limited to Social Media postings and activities, and you consent to such monitoring by your acknowledgment of this policy and your use of the Company’s IT Systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of any and all Electronic Communications and Electronic Information, and other uses of the Company’s IT Systems as well as keystroke capturing and other network or system monitoring technologies.

The Company also may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

Employees are strongly encouraged to use Company IT Systems to communicate with one another for business purposes whenever possible and to refrain from using personal Electronic Devices for business purposes. If you have any questions about the use of personal Electronic Devices for business purposes, including any exceptions from the general rule against the use of personal Electronic Devices for business purposes, please contact HR.

Do not use the Company’s IT Systems for any matter that you desire to be kept private or confidential from the Company.

## **Personal Use of Social Media**

Personal use of Social Media is never permitted on working time. Personal use of Social Media is never permitted at any time by means of the Company’s IT Systems.

**Media contacts**

Employees should not speak to the media on the Company’s behalf without prior permission. All media inquiries should be directed to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

## **Guidelines for Employees’ Responsible Use of Social Media**

The above material covers specific rules, policies and contractual obligations that employees must follow in using Social Media, whether for personal or business purposes, in consideration of their employment and subject to discipline for violations. The following sections of the policy provide employees with common-sense guidelines and recommendations for using Social Media responsibly and safely, in the best interests of the Company. These guidelines are intended to add to, not contradict, limit or replace applicable mandatory rules, policies, legal requirements, legal prohibitions and contractual obligations.

Protect the Company’s Goodwill and Community Reputation. You are personally responsible for what you communicate in Social Media. Remember that what you publish might be available to be read by the masses (including the Company itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

Make it clear in your Social Media activity that you are speaking on your own behalf. Use your personal email address, and not your Company email address, when connecting to Social Media sites for personal purposes or making any personal communications via Social Media.

If you disclose your affiliation as an employee of the Company, it is recommended that you also include a disclaimer that your views do not represent those of your employer. For example, consider such language as “the views in this posting reflect my personal views and do not represent the views of my employer.”

Use good judgment about what you post and remember that anything you say can reflect on the Company, even if you do include a disclaimer. Always strive to be accurate in your communications about the Company. The Company encourages professionalism and honesty in Social Media and other communications.

Respect Copyright and Intellectual Property Laws. For the Company’s protection as well as your own, it is critical that you show proper respect for the laws governing copyright, fair use of copyrighted material owned by the Company or others, trademarks, logos, and other intellectual property, including the Company’s own copyrights, trademarks, intellectual property, and logos.

Respect and Comply With Terms of Use of All Sites You Visit. Do not expose yourself or the Company to legal risk by using a Social Media site in violation of its terms of use. Review the terms of use of all Social Media sites you visit and ensure your use complies with them. If you are using Social Media as part of your job duties, 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) and accompanying Promotional Guidelines specify the terms for businesses administering promotions through Facebook).
* 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 user information the Company collects through the site).
* Requirements for licenses or other permissions allowing use by the site owner and other third parties of the Company’s trademarks or other intellectual property.
* Privacy rights and responsibilities of the site owner and users.

Respect Others. You must comply with the Company’s policy prohibiting harassment, discrimination and retaliation by not posting or sharing anything on Social Media that would violate the Company’s policy, including racial and ethnic slurs, sexist comments, discriminatory comments, or any content that is maliciously false and could therefore be defamatory.

Supervisors should refrain from trying to connect with their subordinates through the use of personal Social Media (for example, making friend requests on Facebook). Neither supervisors nor subordinates should feel pressured to accept or respond to any personal Social Media requests from anyone at the Company.

Employees should refrain from trying to connect with residents and resident family members through the use of personal Social Media (for example, making friend requests on Facebook). No employee should feel pressured to accept or respond to any personal Social Media requests from any resident or resident family member.

**Retaliation Prohibited**

The Company prohibits retaliation against any employee for reporting a possible violation of this policy or for cooperating in an investigation. Any employee who retaliates against another employee in violation of this policy may be subject to discipline, up to and including immediate termination of employment.

## **Conduct Not Prohibited by this Policy**

This policy is not intended to preclude or dissuade employees from engaging in legally protected activities/activities protected by law, including the National Labor Relations Act, such as discussing wages, benefits or other terms and conditions of employment, forming, joining or supporting labor unions, bargaining collectively through representatives of their choosing, raising complaints about working conditions for their own and their fellow employees’ mutual aid or protection or other legally protected activities.

**Employee Acknowledgment**

I have received, read, and understood the Company’s Social Medial Policy. I further understand that I am expected to comply with the Social Media Policy and that, if I have any questions about the Social Media Policy, I should contact HR.

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Name (Please Print)

**LEGAL DISCLAIMER**

AHCA is providing this Social Media Policy Template as a service to its members. This Social Media Template should not be construed as legal advice or opinions on any specific facts. AHCA encourages you to speak with legal counsel before implementing this or any Social Media policies.