COMPUTER, INTERNET, E-MAIL, & SOCIAL NETWORKING POLICY

Heartland Industries, Inc., Hearth Residential Homes, Inc., Adult Life Programs and Montana Achievement Project (All listed companies will be collectively known as "The Company".) refuses to take a back seat to any company in the industry in service to our consumers. Providing that terrific service depends to a very significant extent on the knowledge and skills of our Central Office financial, support and program staff – and we maintain an edge by installing and using the best electronic computing systems available.

The Company, computer and voice communication systems are provided to users for conducting *company business*. Electronic files and communications created, sent, or received through these systems are the property of The Company. The Company reserves the right to monitor computer usage, Internet usage, and communications on the system.

This policy applies to all use by Company employees regarding the Company's electronic data and communication systems. This includes the Company computer network, e-mail and voice mail systems, and all access to or use of the Internet and the local area network.

The Company, reserves the right to access, monitor, and disclose the use of its systems and the contents of files and communications created, sent, or received on the company's systems at any time to determine whether there have been any breeches of security, violations of company policy, or other system misuse. Users have no expectation of privacy in anything they create, store, send, or receive through the Company's computer system.

Authorization
Only authorized Company, employees are allowed to use the computer system, unless management approves access by other parties. In order to discourage unauthorized access, users are encouraged to use system passwords that are difficult to guess.

Confidentiality
Users must exercise special care in handling privileged, proprietary, confidential, or copyrighted electronic files and communications. Any dissemination of such materials must be limited to persons with a legal right to access them.

Without the express direction of his or her supervisor, no employee should attempt to gain access to another employee's documents, programs, or a file without the latter's permission.

Internet Access
All traffic to and from the Internet must travel through the approved internet gateway in order to assure maximum security, virus protection, monitoring, and system management capabilities.

Internet Usage
Except as may be appropriate in electronic communications with employees and customers, users may not send or post messages on the Internet discussing Company, its competitors, or its position on any issue.

Employees are prohibited from using the Company, computer systems and/or the internet while at work to access social networking sites such as, but not limited to, Facebook, Twitter, and/or MySpace for personal use. Employees are similarly prohibited from accessing sites such as YouTube and EBay for personal use. Accessing the aforementioned sites is allowed, if and only if it is for company use such as promoting the company, informing the public of the closing procedure status, or selling company items on the company account on EBay. Express permission must be granted BEFORE using these sites while representing the company."

Virus Protection and Licensing
Due to laws governing the licensing of computer software, no user may install executable files, programs, or utilities onto a company computer without permission of Barb Hillenbrand 320-231-3337.

Any permitted executable files, programs or utilities downloaded or received (by e-mail, floppy disk or other media) from the Internet or other external source must be scanned for viruses and licensed prior to launching. If you require assistance in scanning for viruses or licensing software, please contact Barb Hillenbrand 320-231-3337.

Prohibited Use
Users are prohibited from using the Company, computer systems to send, receive, access, download, display, or print material that is harassing, illegal, sexually explicit, obscene, offensive, defamatory, or disparaging of others based upon their race, color, creed, religion, national origin, sex, marital status, status with regard to public assistance, familial status, disability, sexual orientation, age or other protected class status. Users are prohibited from using the computer system to download copyrighted materials without permission. Users are also prohibited from using the computer system for non-

company commercial purposes or for the transmission of destructive programs, (e.g. viruses or self-replicating code). Prohibited use of the computer system may subject users to disciplinary action up to and including termination, and possible legal action.

Employees also are prohibited from using the Company, computer system and/or the Internet for any unlawful, unethical, or defamatory activities, or any activities that may result in civil action against the company.

Employees should not use nor install their personal computer games, financial software, or other programs on Company's computer system.

E-Mail Policy

This document sets forth the policy of the Company with respect to e-mail. All personnel (including but not limited to employees, consultants, and others working with the Company who use Company's, e-mail system are required to comply with this policy statement.

Business Use. The e-mail system is meant to be used for business purposes of the Company. Limited personal use of email is allowed if (a) in compliance with this policy and (b) is reasonable in amount and does not interfere with work performance or business needs.

Ownership. All email accounts and all information and messages that are created, sent, received or stored on the Company, e-mail system is the sole property of the Company, and are not the property of the employee or other personnel.

E-mail Review. All e-mail is subject to the right of the Company, to monitor, access, read, delete, copy, disclose and use such e-mail without prior notice to the originators and recipients of such e-mail. E-mail may be monitored and read by authorized personnel for the Company for any violations of law, breaches of Company policies, communications harmful to the Company, or for any other reason.

Email Content. Emails should be professional, courteous and in compliance with all applicable laws. Users should employ spell check on all emails sent.

Prohibited Acts**.** Provided below is a non-exclusive list of prohibited acts associated with your use of the Company, email system. When considering the appropriateness of engaging in a particular act, personnel should be guided by both the specific prohibitions and the other mandates set forth in this policy. Prohibited activities include:

- Using any words, images or references that could be viewed as libelous, harassing, illegal, or discriminatory.
- Creating or transmitting email or images that might be considered inappropriate in the workplace, including, but not limited to, messages or images that are lewd, obscene, sexually explicit, or pornographic.
- Creating or transmitting messages or images that might be considered discriminatory, harassing or offensive due to their reference to race, color, creed, religion, national origin, sex, marital status, status with regard to public assistance, familial status, disability, sexual orientation, age or other protected class status.
- Downloading, copying or transmitting documents or software protected by third party copyrights in violation of those copyrights. Any personnel with a question concerning a copyright issue should contact Barb Hillenbrand.
- Using encryption devices and software that have not been expressly approved by the Company.

Security. The e-mail system is only to be used by authorized persons, and personnel must have been issued an e-mail password in order to use the system. Personnel shall not disclose their codes or passwords to others and may not use someone else's code or password without express written authorization from an authorized officer of the Company.

No Presumption of Privacy/Confidentiality. E-mail communications should not be assumed to be private and security cannot be guaranteed. Highly confidential or sensitive information should not be sent through e-mail. Personnel are required to use email in a manner that will not risk the disclosure of Company proprietary and other information to persons outside the Company,

Reporting. Company personnel who are aware of the violation of this policy by another person should report the violation to a supervisor immediately.

Message Retention and Creation. Employees should be careful in creating e-mail. Even when a message has been deleted, it may still exist in printed version, be recreated from a back-up system, or may have been forwarded to someone else. Please note that appropriate electronic messages may need to be saved. The Compay, may be required to produce e-mail in litigation.

Viruses. Any files downloaded from e-mail received from non-Company sources must be scanned with the Company, virus detection software. Any viruses, tampering or system problems should be immediately reported to the computer systems administrator.

Other Policies. All existing Company policies apply to employee conduct in connection with email, including but not limited to, Company policies regarding intellectual property, insider trading, misuse of Company property, discrimination, harassment, sexual harassment, information, data security, and confidentiality.

Passwords. All work-related passwords must be made known to the Company. The use of passwords to gain access to the Company, computer systems or to access specific files does not provide users with an expectation of privacy in connection therewith.

Email Retention. Our computer systems are configured to automatically delete emails after 60-days. If a user has an appropriate reason to keep a copy of the email, the message must be moved to an "'Archive Folder."

Retention in the Event of Litigation, Subpoena, or Regulatory Inquiry. It is Company policy to comply with all legal proceedings. In the event of any litigation, subpoena, regulatory inquiry, criminal proceeding, or the like, Company personnel are absolutely and unequivocally prohibited from deleting, discarding, or destroying any emails or any other documents relating in any way to the litigation, subpoena, regulatory inquiry, criminal proceeding, or the like.

Confidentiality and Social Networking Activities

Heartland Industries, Inc., Hearth Residential Homes, Inc., Adult Life Programs and Montana Achievement Project (All listed companies will be collectively known as "The Company" furthermore.) takes no position on employees' decisions to start or maintain a blog or participate in other social networking activities. However, it is the right and duty of the agency to protect itself from inappropriate activities which may result in unauthorized disclosure of agency and/or consumer information; reflect negatively upon The Company operations and/or consumers; or for other reasons is deemed inappropriate. The Company social networking policy includes rules and guidelines for agency-authorized social networking and personal social networking and applies to all management and staff.

General Provisions

Blogging or other forms of social media or technology include but are not limited to video or wiki postings, sites such as Facebook and Twitter, chat rooms, personal blogs or other similar forms of online journals, diaries or personal newsletters not affiliated with The Company.

Unless specifically instructed, employees are not authorized and therefore restricted to speak on behalf of The Company. Employees may not publicly discuss clients or products, whether confidential or not, outside company-authorized communications. Employees are expected to protect the privacy of The Company and its consumers. Such information includes but is not limited to consumer information, information about employment sites, trade secrets, financial information and business plans.

Employer Monitoring

Employees are cautioned that they should have no expectation of privacy while using the Internet. Your postings can be reviewed by anyone, including the Company. The Company reserves the right to monitor comments or discussions about the agency, its employees, consumers and the industry, including licensing agencies and competitors, which are posted on the Internet by anyone, including current and former employees, and non-employees.

Employees are cautioned that they should have no expectation of privacy while using company equipment or facilities for any purpose.

The Company reserves the right to use content management tools to monitor, review or block content on blogs that violate company blogging rules and guidelines.

Reporting Violations

The Company employees should report any violations or possible or perceived violations to supervisors, managers or the HR department. Violations include discussions of The Company and its employees and clients, any discussion of proprietary information and any unlawful activity related to blogging or social networking.

Discipline for Violations

The Company takes seriously any violations of the social networking policy. For current employees, violation of the agency's social networking policy will result in disciplinary action up to and including immediate termination. With regard to current or former employees who violate the social networking policy, The Company reserves the right to take legal action where necessary against employees who engage in prohibited or unlawful conduct. Legal action may be taken in response to violations which are defamatory or which unlawfully disclose confidential/private information The Company, its services, consumers or other operations.

Personal Blogs

The Company respects the right of current or former employees to use blogs and social networking sites as a medium of self-expression and public conversation and does not discriminate against employees who use these media for personal interests and affiliations or other lawful purposes. Current and former employees are expected to follow the guidelines and policies set forth to provide a clear line between you as the individual and you as a current or former employee.

Bloggers and commenters are personally responsible for their commentary on blogs and social networking sites. Bloggers and commenters can be held personally liable for commentary that is considered defamatory, obscene, proprietary or libelous, or an invasion of privacy by any offended party, including but not limited The Company.

Current employees may not use employer-owned equipment, including computers, company-licensed software or other electronic equipment, nor facilities or company time, to conduct personal blogging or social networking activities.

Current and former employees cannot unlawfully post on personal blogs or other sites the name, trademark or logo of The Company or any business with a connection to The Company without prior permission. Current and former employees cannot post company-privileged information, including copyrighted information or company-issued documents.

Current and former employees cannot post on personal blogs or social networking sites photographs of other employees (when obtained in connection with The Company business or a company-related event), consumers, or vendors, nor can current or former employees post photographs of persons engaged in company business or at company events.

Employees cannot link from a personal blog or social networking site to The Company internal or external web site.

No Waiver. Any delay or failure to discipline personnel for violations of this policy will not constitute a waiver of the Company, rights.

Consequences of Violations. Violations of this policy or other company policies may result in discipline, suspension, termination of employment, and/or legal action.

Questions. If you have any questions concerning these policies, please contact your supervisor otherwise the Company presumes that you understand and will abide by this policy.

I have read the above policies relating to Computer, Internet, E-mail and Social Networking. I understand that the policy applies to both current and former employees The Company and I agree to comply with the policy regardless of whether my employment with The Company terminates for any reason.

_____ _____

Employee Signature Date

_____

Employee Name