BLUE WATER DEVELOPMENTAL HOUSING, INC.
POLICIES AND PROCEDURES: EMPLOYEE INFORMATION

SUBMITTED BY: Jonathan McCulloch	**DATE SUBMITTED:** 02/15/16	**SECTION:** Information Management	
BOARD APPROVED ON: 9/14/16	**DATE REVISED:** 04/18/18	**SUBJECT:** Technology	
ANNUAL REVIEW BY EXECUTIVE DIRECTOR: 04/18/18, 04/17/19, 11/18/20, 04/21/21		**POLICY #:** EE-004	**PAGE #:** 1 of 5

I. APPLICATION

The provisions stated herein shall apply to all employees of the Blue Water Developmental Housing, Inc. (BWDH)

II. DEFINITION

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the organization's business; distracts, intimidates, or harasses coworkers or third parties; or disrupts the workplace.

III. POLICY

It is the policy of the organization that the electronic systems, including computers, fax machines, and all forms of Internet/intranet access, is for this organization's business and for authorized purposes only.

Use of the organization's computers, networks, and internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate organizational purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- Making unauthorized copies of organizational files or other organizational data;
- Destroying, deleting, erasing, or concealing organizational files or other organizational data, or otherwise making such files or data unavailable or inaccessible to the organization or to other authorized users of organizational systems;
- Misrepresenting oneself or the organization;
- Violating applicable laws in any way;
- Engaging in unlawful or malicious activities;

SUBMITTED BY: Jonathan McCulloch	**DATE SUBMITTED:** 02/15/16	**SECTION:** Information Management	
BOARD APPROVED ON: 9/14/16	**DATE REVISED:** 04/18/18	**SUBJECT:** Technology	
ANNUAL REVIEW BY EXECUTIVE DIRECTOR: 04/18/18, 04/17/19, 11/18/20, 04/21/21		**POLICY #:** EE-004	**PAGE #:** 2 of 5

- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the organization's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics;
- Causing congestion, disruption, disablement, alteration, or impairment of the organization's networks or systems;
- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Using recreational games;
- Defeating or attempting to defeat security restrictions on organizational systems and applications;
- Accessing any social media while on duty; including Facebook, Instagram, Twitter, YouTube, etc.;
- Changing any software or hardware without permission from one of the executive team members.

Using organizational electronic systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates the organization's anti-harassment policies and subjects the responsible employee to disciplinary action. The organization's electronic mail system, internet access, and computer systems must not be used to harm others or to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of BWDH resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. The organization will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual internet activities, e-mail use, and/or computer use.

Unless specifically granted in this policy, any non-business use of the organization's electronic systems is expressly forbidden.

If you violate these policies, you could be subject to disciplinary action, up to and including dismissal.

Ownership and Access of Electronic Mail, Internet Access, and Computer Files; No Expectation of Privacy

The organization owns the rights to all data and files in any computer, network, or other information system used in the organization and to all data and files sent or received using any organizational system or using the organization's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. The organization also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the internet and of computer equipment used to create, view, or access e-mail and Internet content. Employees must be aware that the electronic mail messages sent and received using organizational equipment or organizational-provided internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and always archiving by organizational officials. The organization has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with organizational policies and local, state, and federal laws. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate executive team member.

The organization uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems. There is no expectation of privacy in any information or activity conducted, sent, performed, or viewed on or with organizational equipment or Internet access. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on organizational electronic information systems is electronically stored and subject to inspection, monitoring, and evaluation by the organization at any time. Further, employees who use organizational systems and Internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than organizational systems or the organizational-provided Internet access.

The organization has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such

software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action, up to and including dismissal.

Confidentiality of Electronic Mail

As noted above, electronic mail is always subject to monitoring, and the release of specific information is subject to applicable state and federal laws and organization rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software.

It is a violation of this policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others, unless such access is directly related to that employee's job duties. Employees found to have engaged in such activities will be subject to disciplinary action.

Electronic Mail Tampering

Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

Policy Statement for Internet/Intranet Browser(s)

The internet is to be used to further the organization’s mission, to provide effective service of the highest quality to the individuals served, and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of internet/intranet access are organizational resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Employees are individually liable for any and all damages incurred as a result of violating organizational security policy, copyright, and licensing agreements.

All organizational policies and procedures apply to employees' conduct on the internet, especially, but not exclusively, relating to intellectual property, confidentiality, organizational information dissemination, standards of conduct, misuse of organizational resources, anti-harassment, and information and data security.

SUBMITTED BY: Jonathan McCulloch	**DATE SUBMITTED:** 02/15/16	**SECTION:** Information Management	
BOARD APPROVED ON: 9/14/16	**DATE REVISED:** 04/18/18	**SUBJECT:** Technology	
ANNUAL REVIEW BY EXECUTIVE DIRECTOR: 04/18/18, 04/17/19, 11/18/20, 04/21/21		**POLICY #:** EE-004	**PAGE #:** 5 of 5

Personal Electronic Equipment

Due to the significant risk of harm to the organization's electronic resources, or loss of data, from any unauthorized access that causes data loss or disruption, employees should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, USB / flash drives, "smart" phones, iPods/iPads/iTouch or similar devices, laptops or other mobile computing devices, or other data storage media) to the workplace and connect them to the organization's electronic systems unless expressly permitted in writing to do so by the organization. To minimize the risk of unauthorized copying of confidential business records and proprietary information that is not available to the general public, any employee connecting a personal computing device, data storage device, or image-recording device to organizational networks or information systems thereby gives permission to the organization to inspect the personal computer, data storage device, or image-recording device at any time with personnel and/or electronic resources of the organization's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the data-storage device in question in order to ensure that confidential business records and proprietary information have not been taken without authorization. Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not connect them to organizational computers or networks.

Violation of this policy, or failure to permit an inspection of any device under the circumstances covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment, depending upon the severity and repeat nature of the offense. In addition, the employee may face both civil and criminal liability from the organization, from law enforcement officials, or from individuals whose rights are harmed by the violation.