



**POLICY:** Acceptable Use **DEPARTMENT:** ALL  
**APPROVED:** Robert W Stinson **REVIEWED / REVISED:** 10/15/14

### 1.0 Purpose

The computing resources at the Hannibal Board of Public Works (HBPW) support the administrative activities of the HBPW and the use of these resources is a privilege that is extended to employees or contractors of the organization. As a user of these services and facilities, you have access to valuable HBPW resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, HBPW will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the HBPW. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

This document establishes specific requirements for the use of all computing and network resources at the HBPW.

### 2.0 Scope

This policy applies to all users of computing resources owned or managed by HBPW. Individuals covered by the policy include (but are not limited to) staff, guests or contractors, external individuals and organizations accessing network services via HBPW's computing facilities or remotely.

Computing resources include all HBPW owned, licensed, or managed hardware and software, and use of the network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

#### 2.1 Rights and Responsibilities

As an employee of the HBPW, the HBPW provides you with the use of work-related tools, to certain computer systems, servers, software and databases, to the telephone and voice mail systems, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy, and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of the HBPW that apply to appropriate use of the HBPW's technologies and resources. You are responsible for exercising good judgment in the use of the technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

As a representative of the HBPW, you are expected to respect the HBPW good name in your electronic dealings with those outside the organization.

### 3.0 Policy

Policy Sections Include:

### **3.1 Acceptable Use**

- 3.1.1** You may use only the computers, computer accounts, and computer files for which you have authorization.
- 3.1.2** You may not use another individual's account, or attempt to capture or guess other users' passwords.
- 3.1.3** You are individually responsible for appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware. Therefore, you are accountable to the HBPW for all use of such resources. As an authorized HBPW user of resources, you may not enable unauthorized users to access the network by using a HBPW computer or a personal computer that is connected to the network.
- 3.1.4** The HBPW is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.
- 3.1.5** You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access.
- 3.1.6** You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system administrator.
- 3.1.7** You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- 3.1.8** You must not use HBPW computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.
- 3.1.9** On HBPW network and/or computing systems, do not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless you have been specifically authorized to do so.

### **3.2 Fair Share of Resources**

Administrators of the HBPW which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The network, computer clusters, mail servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others in the organization is explicitly forbidden.

The HBPW may choose to set limits or restrictions on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

### **3.3 Adherence with Federal, State, and Local Laws**

As a member of the HBPW, you are expected to uphold local ordinances and state and federal law. Some HBPW guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

As a user of HBPW's computing and network resources you must:

- Abide by all federal, state, and local laws.

- Abide by all applicable copyright laws and licenses. HBPW has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.
- Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.
- Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

### **3.4 Other Inappropriate Activities**

Use HBPW's computing services for those activities that are consistent with the educational, research and public service mission of the HBPW. Other prohibited activities include:

- Activities that would jeopardize the HBPW's tax-exempt status
- Use of HBPW's computing services and facilities for political purposes
- Use of HBPW's computing services and facilities for personal economic gain

### **3.5 Privacy and Personal Rights**

- All users of the HBPW's network and computing resources are expected to respect the privacy and personal rights of others.
- Do not access or copy another user's email, data, programs, or other files without permission.
- Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to discipline as well as legal action by those who are the recipient of these actions.

While the HBPW does not generally monitor or limit content of information transmitted on the network, it reserves the right to access and review such information under certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that HBPW is not subject to claims of misconduct. In addition, because HBPW is a municipal entity, certain information may also be subject to public disclosure pursuant to the Missouri Sunshine Law. Employees should understand that there is no reasonable expectation of privacy in electronic data accessed or stored on HBPW networks or systems.

Access to files on HBPW-owned equipment or information will only be approved by specific personnel when there is a valid reason to access those files. Authority to access user files can only come from the Administrator in conjunction with requests and/or approvals from senior members of the organization. External law enforcement agencies may request access to files through valid subpoenas and other legally binding requests. Information obtained in this manner can be admissible in legal proceedings.

#### **3.5.1 Privacy in Email**

While every effort is made to insure the privacy of HBPW email users, this may not always be possible. In addition, since employees are granted use of electronic information systems and network services to conduct HBPW business, there may be instances when the HBPW, based on approval from authorized staff, reserves and retains the right to access and inspect stored information without the consent of the user. Please see HBPW's Electronic Mail Policy for further details.

### **3.6 User Compliance**

When you use HBPW computing services, and accept any HBPW issued computing accounts, you agree to comply with this and all other computing related policies. You have the responsibility to keep up-to-date on changes in the computing environment and to adapt to those changes as necessary.

### **3.7 Offsite Use of HBPW Equipment**

Members of the HBPW may need to have access to technology related equipment while outside of the office. This equipment can be loaned out on an as needed basis or on a permanent issue basis. While the equipment is in the possession of the HBPW employee, they are to use the equipment for its intended purpose and continue to adhere to this and all HBPW policies.

- 3.7.1** If the device is equipped with means to connect to the internet in any fashion, precautions should be taken to ensure the connection and the traffic sent across the connection are traveling across a secure network. Using public wifi connections or connections that do not require authentication through a secure username and password should not be used. If the device is equipped with a cellular connection device, it is advised to use this when there is a need for connectivity in a questionable location.
- 3.7.2** Company cellular data plans are limited on monthly usage and are shared among multiple members of the organization. Use this connection method when necessary but ensure it is disabled when not in use.

### **3.8 Use of HBPW Internal Network From Personal Device**

The connecting of any personal computer to the corporate network for any reason is prohibited. If an employee wishes to connect his/her personal device to the internal wireless network, the network administrator should be contacted. Please note when a personal device is connected to the company network, all content on that personal device could be subject to Missouri Sunshine Law requests and all information contained on or transmitted to / from that device is subject to review.

While on HBPW property or at a HBPW worksite, employees may not use personal devices for any purpose that violates the law or HBPW policy, including sending, storing, or viewing unlawful, offensive, discriminatory, harassing or other inappropriate materials, regardless of whether the device is connected to any HBPW wired or wireless network or an employee's personal data account.

### **3.9 Social Networking**

Some employees of the HBPW have job related roles that give them the authority to post to social networking sites on behalf of the HBPW for public announcements of various types. The use of social networking during scheduled working hours from any HBPW equipment or while connected to the internal wireless network, is discouraged. Employees may not post or display comments, photographs, video, or audio about other employees or customers or the HBPW that could be viewed as vulgar, obscene, threatening, intimidating, harassing, or a violation of the HBPW's policies against discrimination and or harassment or hostility based on age, race, religion, sex, ethnicity, gender, nationality, disability, or other protected class, status or characteristic. Activity of this type is subject to review at any time and management of the HBPW can take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the HBPW.

Nothing in this policy is intended or should be interpreted to limit the rights of employees' rights under Section 7 of the National Labor Relations Act.

## **Examples of Acceptable Use**

The following scenarios are intended to provide examples of acceptable and unacceptable uses of HBPW's computing resources, based on the Acceptable Use Policy. These examples are not comprehensive but are merely illustrations of some types of acceptable and unacceptable use.

## **Authorized Use**

### **Acceptable:**

- While using someone else's computer from outside the office, you connect to HBPW to check your email. When you have finished, you log off of your account, closing any browser windows you may have used, and making sure your email password was not saved on the computer.
- While traveling on vacation, you ask a staff person to check your email for you by forwarding your email to their account, removing the forwarding on your return.

### **Unacceptable:**

- While someone else is using a computer, you want to check your email. You ask them to log in, giving them your password to type in for you.
- While traveling on vacation, you ask a staff person to check your email for you by giving them your password.
- A colleague is out sick, and he/she was receiving responses for an event. Rather than calling them at home to ask them to check their email, you attempt to gain access to their account by guessing their password.
- After having your computer hacked, you decide to download and run hacking tools yourself to help your friends out by checking for vulnerabilities on their computers.

## **Fair Share of Resources**

### **Acceptable:**

- You conduct a secure remote sharing session with a vendor using your computer.
- You use a shared computer in the office that you are authorized to use.

### **Unacceptable:**

- While using a computer on the network, you alter its setup, so that each time it starts up, your favorite programs are started automatically.
- As an employee at HBPW, you store your photos, music, movies or unauthorized software on HBPW resources (either on your workstation or a HBPW server).

## **Adherence to Laws**

### **Acceptable:**

- Storing legitimately-obtained files for instructional use.
- Displaying a legally reproduced copy (with copyright notice) of a videotaped presentation for instructional purposes.

### **Unacceptable:**

- Taking a CD you own, you make copies of songs onto your computer, and set up sharing to allow others to access those songs from your computer.
- Playing a video for entertainment purposes unrelated to HBPW normal activity on a computer.

## **Other Inappropriate Activities**

- Using a computer connected to HBPW's network, you establish a commercial business, selling products or services over the Internet.
- You download, store, print and/or display materials that could be perceived by others as contributing to an intimidating, hostile, or sexually offensive working environment.
- You send out unauthorized and unsolicited email messages to other HBPW employees.

## **Privacy and Personal Rights**

### **Acceptable:**

- As part of an investigation into an employee's potential misuse of the network for copyright violations, permission is granted from an appropriate office for a supervisor to log into that employee's computer and check files that are stored on it.

### **Unacceptable:**

- While checking the email system for possible problems, a systems staff person has to open a mailbox owned by someone else. In doing so, he or she reads the subject lines, finds one that looks interesting, and opens the email message.

## **User Compliance**

### **Acceptable:**

- When accepting an offer for employment, the employee reads the issued policy, agrees to it, and signs.
- As malware alerts and other news are sent from the network administrator, an individual takes appropriate action to protect his or her computers from those threats.

### **Unacceptable:**

- When an employee signs a policy without reading it or if prompted on the screen, an individual quickly clicks on the "I Agree" button without reading the policy or acknowledging responsibility for following it.
- Ignoring suggestions or instructions from the network administrator.

## **Originated / Revised History**

Originated – 07/05/02

Revision 1 – 09/23/02

Revision 2 – 10/18/02

Revision 3 – 12/16/02

Revision 4 – 06/29/09

Revision 5 – 08/07/09

Revision 6 – 06/27/14

Revision 7 – 10/15/14

Revision 8 – 11/17/14

# Acceptable Use Policy

All Hannibal Board of Public Works employees who have a valid need to access any or all information systems in the facility are required to abide by the Acceptable Use Policy.

Complete the section below and submit a signed copy to your supervisor.

I have read and understand and agree to abide by the Hannibal Board of Public Works Acceptable Use Policy

**Employee Name – Printed**

---

**Employee Signature**

---

**Today's Date**

---

**Supervisor Signature**

---

(This document shall be retained in each employee's personnel file.)