Hawkeye Area Community Action Program, Inc.	Policy # 515
	Page 1 of 4
Use of HACAP Computers, Equipment and Information Systems	
	Effective: April 25, 2019
APPROVED BY: HACAP Board of Directors	**Revised: May 25, 2023**

Policy Statement

HACAP employees are assigned agency computers and other electronic devices to perform their daily work functions. HACAP provides access to the agency network for employees that include email and internet usage. Access to computer systems/electronic equipment and the network imposes certain responsibilities and obligations. Appropriate use should be legal, ethical, reflect agency and community standards and show restraint in the consumption of shared resources.

EMAIL USAGE

HACAP's email system has been provided to help employees communicate with each other, consumers, vendors and other agencies. Email users should adhere to all company standards of decency and should not abuse the resources that are available to them.

INTERNET USAGE

HACAP provides access to the internet for staff to do their job Internet access for HACAP is a business tool, provided to you at HACAP's cost. HACAP expects you to use the internet for business related purposes, to research relevant topics and obtain useful business information. This policy must be followed in conjunction with other HACAP policies governing appropriate workplace conduct and behavior.

Standard Operating Procedure

General Network Usage

1. Every authorized user retains his/her own password for access to the network, passwords will initially be set by the Information Systems Department and subsequently changed by the user on their first log in to the network. Users will be required thereafter to change their passwords according to the schedule set by the Information Systems Department. All users are prohibited from the unauthorized access to other users' files, email messages and passwords. Disregarding this policy may result in disciplinary actions. Users should treat any password as confidential information. Users are prohibited from attempting to circumvent or subvert any HACAP security measures. Intentional action designed to circumvent any HACAP security system is grounds for disciplinary action.
2. Passwords for any HACAP systems or programs are not to be disclosed either intentionally or accidentally. Avoid writing your password down and never leave your password on notes affixed to your screen or other items in your work area. A user name and password for any system accessed for HACAP use are issued to you for your personal use and must

never be communicated to another person. If network or program access is needed for temporary or part-time employees, please contact the network administrator to receive a user name and password.

3. Although each user has an individual password to access this system, the computer and any data it contains belong to HACAP. Each user is given access rights to specific files and software applications. HACAP management reserves the right to inspect all files stored on our network or any computer in order to assure compliance with these policies. This includes the HACAP network, individual computer storage areas and any company owned storage media, including data backups.
4. Every authorized user is responsible for the protection of confidential information from unauthorized uses. All users are prohibited from the unauthorized access of confidential information regarding employees or clients outside the information needed for the user to complete their assigned job responsibilities.
5. No software can be installed, copied or used on HACAP computers without the knowledge and permission of the Information Systems Department. All software must be properly licensed, and all license provisions must be strictly adhered to. As a result, individual users may not install software brought from home or downloaded from the internet. User installed screen savers are allowed, if they are not visually offensive, and they meet all previously defined licensing guidelines. In all circumstances, the Network Administrator will determine if any software meets HACAP licensing requirements.
6. HACAP equipment is meant for the employees' business use and not the use of family members either at work or when taken home. Users are not allowed to install or play games on any HACAP-owned computer systems, unless it is approved educational software for use in the Head Start classrooms.
7. Company owned software is not to be taken home by employees, unless licensing specifically allows for employee use at home.
8. The display of any kind of sexually explicit image or document on any company system is prohibited. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or technical resources.
9. HACAP's computer systems should not be used, under any circumstance, to libel, slander or harass another person, as defined in company policies.
10. The Network Administrator may access the files or others for the maintenance of networks, computers and storage systems, such as to create a system backup.
11. Users should regularly review personal and departmental files, deleting any files that are no longer necessary. Network storage space involves a financial investment to HACAP and

as such, file storage must be regularly reclaimed to make space available for other users and information.

E-Mail

1. All email messages are company records. The content of any email message may be disclosed within the company to management without your permission and without your knowledge. Therefore, you should not assume that email messages are confidential. HCAP maintains a policy of backing up and maintaining data files and email messages, this applies to messages and files that you have deleted. Deleting an email message or a file does not guarantee that it has been erased from the system.
2. HACAP provides the electronic mail system to assist you in the performance of your job; you should use it for appropriate HACAP business. Incidental and occasional personal use of email in permitted, but these personal messages will be subject to the review as other messages. Since your personal messages can be accessed by management without prior notice or permission you should not use email to transmit any messages you would not want read by a third party.
3. Be aware of "phishing emails" coming from unknown or even know users asking you to access something through a link or provide them with any personal information. These emails may come from someone on your contact list or within HACAP. If the request seems out of place or if the email address on the "From" information does not match the user email address, do not reply. Delete the email and empty your deleted emails to make sure it is not available. If you are unsure, forward it to IS Desk.
4. User should regularly review and discard messages that are no longer needed. This includes any items in user's personal folder, sent items and Inbox. Once deleted you will need to empty the "Deleted Items" folder to clear the messages from your Outlook. Each user does have a limited amount of storage for their email and the system will message you when it is becoming full and emails can no longer be sent or received.

Internet

1. HACAP limits the use of E-Mail, the internet and other access privileges to those employees who have legitimate business need. While incidental personal use is permitted engaging in non-work-related use of any HACAP equipment is prohibited.
2. Unnecessary or unauthorized internet usage causes network and server congestion. It may slow other users, it takes away work time, consumes supplies, and ties up printers and other shared resources. Unlawful internet usage may also bring about negative publicity for the company and expose HACAP to significant legal liabilities.

3. Social sites, chats, newgroups and email distribution list give each individual internet user an immense and unprecedented ability to propagate information. Instant access to all information, both that in the public domain ad well as highly confidential information can cause incredible liability risk both to the individual employee as well as the agency. Because of that power, we must take special care to maintain the clarity, consistency, and integrity of HACAP's agency image. Anything anyone writes on the internet in the course of acting for the company can be taken as representing a HACAP position. Posting information to wide-scale distribution lists or other mass communication vehicles should be highly scrutinized and cleared with a supervisor before release.
4. HACAP has software in place that allows for monitoring and recording of all internet usage. We want you to be aware that HACAP has record (for each and every user) each internet site visited, each chat, each email message and each file transfer into and out of our internal networks. No employee should have any expectation of privacy as to his or her internet usage. This monitoring will be done by the Network Administrator or the Deputy Director on a random basis or at a supervisor's request. Any misuse of the system will be shared with the employee's direct supervisor and the CEO.
5. This HACAP policy will be distributed and signed for new employees at the New Employee Orientation.

Process Manager

The Deputy Director implements the Use of Computers, Equipment and Information Systems Procedures.

Target Audience

All HACAP employees.

Necessities

Any HACAP employee that uses a HACAP computer

Process Manager

This policy was written by the Information Technology Department for use by all HACAP operations. Questions regarding this policy should be directed to the Information Technology Department at 319-393-7811.