## GENERAL

The purpose of this policy is to ensure the proper use of EHSD furnished computer equipment, internet, e-mail and other electronic communications systems and to make users aware of acceptable and unacceptable use of these systems. EHSD reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

All electronic appliances including personal computers, laptop computers, cell phones, Personal Data Assistant (PDA), Blackberrys, and pagers are provided by EHSD to allow employees to efficiently conduct official business in support of EHSD, Contra Costa County and the clients we serve.

E-mail is an official business communications tool and users must use this tool in a responsible, respectful, effective and lawful manner to carry out their official duties. EHSD provides Internet and Intranet access, computer systems and networks for lawful official business purposes. Use of all EHSD systems including the Internet or Intranet is subject to monitoring for appropriate use, security and/or network management and employees may be subject to limitations on their use of such resources.

Employees are responsible for safeguarding the Department’s sensitive data, information and records. Employees work with both paper and electronic records and computer systems. In addition to ensuring that all paper records are properly handled, secured and disposed of, this policy also spells out expectations for computer and electronic device security as well as policies related to PCs used for County-work purposes at work sites, remote sites (laptops) and home, as well as Internet and email usage. Employees must immediately report to their supervisor the theft or loss of any electronic device that was furnished by EHSD or Contra Costa County including portable storage devices such as computer disks and flash drives. Employees must also immediately report the theft or loss of any paper or electronic records that contain personal, private, or confidential information about clients or employees.

These policies apply to all employees who have access to EHSD computer systems or networks, are provided an EHSD or County issued computer to carry out EHSD business, or who have access to data emanating from EHSD data bases or records. Contractors and employees of contracting agencies who have access to EHSD data will be informed of these policies and are expected to conform to the intent of the policies. All new permanent and temporary employees, contractors and employees of contracting agencies will be required at the beginning of their tenure to read and sign this document. All current employees will be provided a copy of this document by their immediate supervisor, who will be required to document its specific transmission and provide that documentation to the Department Personnel Unit.

II. REFERENCES

* + County Computer system employee responsibility statement, 01/01/1996
	+ Confidentially Statement (ADM 10)
	+ Electronic Email, County Administrative Bulletin 139
	+ Internet Usage, County Administrative Bulletin 140

III. POLICIES

1. E-mail Usage

As a user of EHSD e-mail you are expected to adhere to all applicable laws and the following policies. Users will not:

1. Initiate or forward e-mails containing profanity, libelous, defamatory, offensive, racist, vulgar, or obscene remarks, photos, cartoons, or jokes. Prompt notification to the supervisor is required if an e-mail of this nature is received.
2. Forge or attempt to forge e-mail messages.
3. Misrepresent an e-mail written by another person by altering and sending it to a third party, giving the impression that the originator wrote the altered version without the express approval of the originator.
4. Disguise or attempt to disguise your identity when sending e-mail.
5. Send e-mail messages using another person’s e-mail account without authorization.
6. Use e-mail for any illegal purpose.
7. Use the EHSD e-mail for any commercial purpose not related to official business.
8. Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of EHSD without specific approval.
9. Send unsolicited e-mail messages that consist of junk mail, chain letters, or advertising material to EHSD employees or from EHSD equipment.
10. Participate in any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
11. Create or forward chain letters, Ponzi schemes or pyramid schemes of any type.
12. Post the same or similar nonbusiness-related messages to large numbers of Usenet newsgroups (newsgroup spam).
13. E-mail encryption

Users may not encrypt any e-mails without obtaining written permission from a manager at the Division Manager level or higher. If approved, the encryption key(s) must be made known to EHSD.

C. E-mail retention

E-mails should be deleted after 90 days. If a user has sufficient reason to keep a copy of an e-mail, the message should be moved to a folder for Archiving. Power users may request approval from their Bureau Director for longer term or higher volume retention of e-mail in their active files.

D. E-mail accounts

All e-mail accounts maintained on our e-mail systems are property of EHSD. E-mail accounts not used for 180 days will be deactivated and possibly deleted. E-mail accounts for former employees will be deactivated upon departure.

E. E-mail disclaimer

All Department networks will be programmed to append the following disclaimer to each e-mail that includes one or more addressees outside of EHSD:

“The information contained in or accompanying this e-mail is intended only for the use of the stated recipient(s) and may contain information that is confidential and/or privileged. If the reader is not the intended recipient or the agent thereof, you are hereby notified that any dissemination, distribution or copying of this e-mail is strictly prohibited and may constitute a breach of confidentiality and/or privilege. If you have received this e-mail in error, please notify the sender immediately. Any views or opinions presented are solely those of the author and do not necessarily represent those of Contra Costa County.”

F. Internet / Standard usage / security

The following activities, some of which may be violations of laws, are strictly prohibited, with no exceptions:

1. Internet

1. Visiting or attempting to visit internet sites that contain illegal, obscene, sexual, racial, religious, or hateful content which is objectionable and inappropriate for the workplace.
2. Using any browser except Internet Explorer which is the only authorized web browser in the EHSD Network. No other web browser is permitted to be used.
3. Standard usage
	1. Providing information about, or lists of, EHSD clients or employees to parties outside the EHSD without specific authorization.
	2. Engaging in any activity that is illegal under local, state, federal or international law while utilizing the EHSD owned resources.
	3. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by EHSD.
	4. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the EHSD, or the end user does not have an active license.
	5. Unauthorized copying, forwarding, deleting, altering, or attempting to limit access to intellectual property of EHSD including such materials as policies, procedures, processes, presentations, grants and training materials.
	6. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. Employees should consult with their Bureau Director prior to the export of any material that is in question.
	7. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)
	8. Making fraudulent offers of products, items, or services from any EHSD account or equipment.
	9. Storing personal high volume files such as music or photographs on EHSD computers or the network.
4. Security

Breaching network security, disrupting network communications or unauthorized access to data or unauthorized access to all or part of the network is prohibited. Security breaches include, but are not limited to:

1. Accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless doing so is within the scope of the employee’s duties and is done for an authorized purpose. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
2. Port scanning or security scanning.
3. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal duties.
4. Circumventing user authentication or security of any host, network or account including circumventing or attempting to circumvent EHSD firewalls or filters.
5. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
6. Using any program, script, command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
7. Personal Use

It is strictly forbidden to use the EHSD Internet or e-mail system for anything other than legitimate official business purposes. Occasional and short incoming or outgoing unofficial e-mail messages are permitted provided they comply with all other EHSD e-mail policies. Occasional or infrequent Internet searches for information generally done during nonworking time are also permitted provided such searches comply with all other EHSD Internet policies. Employees will not use EHSD systems for any commercial or unofficial business purposes, including such things as personal businesses for profit or nonprofit, involvement with outside groups including service or religious groups. The transmission of personal e-mails (except occasional and short), chain letters, junk mail, jokes and executable files is prohibited. All messages distributed via EHSD’s e-mail system are EHSD property and may be accessed at any time by authorized EHSD representatives for security or other authorized purpose.

1. Cell phone Usage

Communication equipment, including Personal Digital Assistant (PDA), cell phones and other telecommunication devices, are provided for employees to conduct official County business. The Department will provide specific equipment or services based on job necessity.

Users of cell phones, PDAs and other portable communications devices must comply with safe practices and all applicable state laws, especially with operating a County-owned vehicle or a personal vehicle while conducting County business. Employees are strongly encouraged to safely pull to the side of the road when making or receiving calls on portable communications devices while driving.

The use of County-issued cell phones and/or communication devices, such as Blackberrys, PDA or Smartphones is regularly monitored. Upon request, copies of employee cell phone billing statements will be made available to senior management for purposes of review. Employees issued County communications equipment are expected to reimburse the County for any and all communication fees accrued by personal use.  Personal use is strongly discouraged except for serious emergencies, and will be monitored by the Department. Excessive personal use while on official duty will result in supervisory action, including but not limited to loss of privileges with regards to the use of communications equipment and/or possible disciplinary action up to and including termination of employment.

I. Use of Portable Electronic Devices

Employees are not to use personal laptops, personal cell phones or other personal portable communications devices, portable DVD players or other devices such as radios or iPod’s in their work areas when doing so may interfere with their own work performance or the work performance of others. Personal television sets or devices that provide television coverage are also prohibited.

1. Confidential Information

Great care must be used in sending confidential, personal, or private information via e-mail, cell phone or PDA. This information could include client or employee names, home addresses, home phone numbers, dates of birth, Social Security Numbers, criminal history, income or asset information, medical information, or other sensitive information. Generally, such information should be sent encrypted and only to a receiver who has an authorized need for the information. If in doubt as to whether to send certain information via e-mail, employees should get clarification and approval from an appropriate supervisor before sending the information. Employees must also exercise great care before downloading sensitive information to a laptop computer, or portable storage devices such as disks or flash drives since such portable devices are subject to being lost or stolen. Data stored on portable devices should be password protected and encrypted.

1. Passwords

Authorized users are responsible for the security of their passwords and accounts. Passwords, including network, CalWIN and other system passwords, should not be revealed to others. Any exceptions to sharing passwords must be approved by an appropriate manager. All passwords must be made known to a designated EHSD staff person, generally a supervisor or manager. The use of additional, self-initiated passwords to block access to computer systems or to secure specific files is not authorized without specific approval, and does not provide users with an expectation of privacy in the respective system or document. EHSD IT Division will notify each user when a password update is to be performed. System-level passwords should be changed quarterly and user-level passwords should be changed every six months or as established by the state.

L. System Monitoring

While use of the EHSD network provides a reasonable level of privacy, users should be aware that the data they create, receive and/or store on county systems becomes and remains the property of the EHSD. Because of the need to protect the integrity of the EHSD network, this policy serves as notice to all employees that they cannot expect and management cannot guarantee the confidentiality or privacy of information stored on any electronic devices belonging to or furnished by the EHSD.

Users expressly waive any right of privacy in anything they create, store, send or receive on EHSD’s computer systems. For security and network maintenance purposes, authorized individuals within EHSD may, at any time, and without prior notification, monitor or audit the use of equipment, systems and network traffic and may do so on a periodic basis to ensure compliance with this policy. If there is evidence that these policies are not being adhered to, EHSD reserves the right to take action, including disciplinary action up to and including termination and/or legal action.

M. General Usage Guidelines

The following guidelines areto identify activities that are considered acceptable or unacceptable uses or practices:

1. EHSD issued Blackberrys or any other PDA devices should be password protected to prevent unauthorized access to the phone and e-mail features in case the Blackberry or other PDA device is lost or stolen.
2. All PCs, laptops, personal workstations used to conduct official EHSD business and portable storage devices should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, by logging-off (control-alt-delete for Win2K users) when the host will be unattended, or appropriate and approved encryption to protect data.
3. Information on portable computers and portable storage devices such as disks and flash drives is especially vulnerable to unauthorized access or the theft or loss of the computer or device. Users of EHSD-issued laptops and storage devices must exercise special care to secure laptops and storage devices and to not leave them unattended.
4. Unless specifically authorized by an appropriate management official for a work purpose, employees are not to make postings to newsgroups from an EHSD e-mail address since to do so could imply that the views expressed may be official EHSD policy.
5. All electronic devices used by the employee that are connected to the EHSD Internet/Intranet/Extranet, whether owned by the employee or the EHSD, must continually execute approved virus-scanning software with a current virus database.
6. Except as specifically exempted by a Bureau Director or equivalent, data on an EHSD PC is to be stored on network drives (Global drives or your H: drive (Home Directory)) and not on the local drive. Data on network drives can be accessed through the use of the secured (encrypted) VPN (virtual private network) token. The network storage is secure, and backed-up. Data stored on a local drive of a laptop or desktop PC has virtually no security, and are not backed up by the department. Any data authorized to be stored on a local drive must be periodically backed up by copying to a separate portable storage device. Employees must, except as specifically authorized, use the secured network drive to access data, versus the local drive.
7. Employees must use extreme caution when opening e-mail attachments received from unknown senders. Such attachments may contain viruses, e-mail bombs, or Trojan horse code. When in doubt, delete the e-mail without opening, or call the IT Help Desk for guidance.
8. All data, correspondence, documents, and materials, whether printed or electronic, prepared on EHSD owned or furnished equipment or prepared as part of an employee’s official duties are the sole, specific and intellectual property of the Department. Destruction or removal, failure to safeguard and back up documents, and/or unauthorized transmission of any such information or documents not authorized by this policy or the staff person’s immediate supervisor is prohibited. Unauthorized destruction or removal of documents will be considered theft or malicious destruction and will subject the staff person to disciplinary action, up to and including dismissal, as well as possible legal action.

N. Employee Certification Required

Upon hire, each employee of the department is required to sign the County Computer System Employee Responsibility Statement (County-wide Standard) and the Confidentially Statement (ADM 10). These documents certify that the employee has read and understood these policies as well as the confidentiality policies and will be held responsible for knowledge of these policies. Contractors and employees of contracting agencies will be asked to read and understand these policies and sign the declaration below statement certifying that they have read and they understand these policies. Employees and employees of temporary services agencies will sign the below declaration as part of their orientation or processing in the EHSD Personnel Office. For other contractors, the Contract Requesting Party, i.e., the EHSD employee or manager who requested the contract, will have the contractor sign the declaration before the contractor begins work.

O. Best Practices

1. EHSD’s e-mail style is informal. Sentences can be short and to the point and an e-mail message can start with ‘Hi’, or ‘Dear’, and the name of the person. Messages can be ended with ‘Best Regards’. The use of Internet abbreviations and characters such as smiley faces is not encouraged.
2. Users should do a spell and grammar check of all e-mails prior to transmission.
3. Do not send unnecessary attachments. Consider the impact on the network before sending large attachments, e.g., those larger than 200K.
4. Do not write e-mails in all capital letters.
5. Keep e-mail messages short and respectful.
6. Do not engage in excessive e-mail exchanges on the same topic; determine if matters would be better resolved by phone or by a meeting.
7. Do not blind copy someone when doing so is intended to embarrass the recipient of the e-mail.
8. Ensure the e-mail is addressed to the proper recipient and especially if there is more than one person with the same name, so that only the intended people receive the e-mail.
9. Ensure that e-mail that is not intended to be forwarded is not forwarded.
10. Send your e-mail to the minimum number of addressees. Avoid “Reply to All” when a response to a smaller number of recipients is more appropriate.
11. Delete unnecessary e-mail from your system.

P. Enforcement

Any employee found to have violated any of the policies set forth above may be subject to disciplinary action, up to and including termination of employment.

Q. Declaration

I have read, understand and acknowledge receipt of the Information Technology Policy. I will comply with the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action, up to and including termination of my employment. If I am a contractor or an employee of a contracting agency, my signature means that I have read and I understand the policies above and there could be consequences to my contractor status if these policies are not followed.

CONTACT PERSON: First-line supervisors and above may contact the Administration Bureau Information Technology Manager or his/her designee with questions about this department manual section.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Signature: |       |  | Date: |       |
|  |
| Printed Name: |       |  |  |  |

Definitions

Term Definition

Contractors Contractors discussed in this policy are companies and individuals including employees of temporary services agencies, having access to EHSD systems or data.

EHSD Refers to the Employment and Human Services Department and all Bureaus within this Department including Workforce Services, Adult and Aging, Children’s Services, Community Services, Administration, as well as other entities supported by EHSD through its computer networks or the issuance of computer equipment or other electronic devices.

E-mail Bomb An email bomb is a way to deny someone access to his email account for a period of time.

Employees As used in this policy, employees refers to all full-time, part-time, permanent and temporary county employees.

Extranet An extranet is a private network that uses Internet technology and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses.

FTP Stands for File Transfer Protocol. It is used to make files and folders publicly available for transfer over the Internet (\*A protocol is a language that enables computers to speak to one another \*) Win2K Windows 2000 Operating System

Intranet An intranet is a private network that is contained within an organization uses internet technology to share internal resources.

Internet A worldwide system of interconnected computer networks

Network Sniffing Inspecting network traffic at a very detailed level

Packet Spoofing Forging the originator of network traffic; to impersonate

Pinged Floods To overwhelm with nonsense requests (see ‘Service Attack’ below)

Service Attack To overwhelm a network with nonsense requests

Smiley Using letters or icons to convey emotions in emails

Spam Unauthorized and/or unsolicited electronic mass mailings.

Trojan Horses A destructive program that masquerades as a benign application.

Virus A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.

Worms A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.