CAMPBELL COUNTY HEALTH
INFORMATION TECHNOLOGY DIVISION
ADMINISTRATION POLICY & PROCEDURE

SUBJECT: ACCEPTABLE USE

OVERVIEW:

A. The intention for publishing this Policy is not to impose restrictions that are contrary to our established culture of openness, trust and integrity. Understanding and adhering to this policy is necessary in order to protect our employees and Campbell County Health (CCH) from illegal or damaging actions by individuals, either knowingly or unknowingly.

B. Effective security is a team effort involving the participation and support of every CCH employee, provider, contractor and vendor who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

OBJECTIVE:

To outline the minimum acceptable use of computer equipment, email, and internet access at all CCH locations. These rules are in place to protect the employee and the hospital. Inappropriate use exposes CCH to risks including virus attacks, compromises of network systems and services, and legal issues.

PROCEDURE:

A. General Use and Ownership
   1. All information security responsibilities shall be defined and allocated.
   2. Employees should be aware that the information they create or store using CCH owned systems is the property of CCH. Therefore, Management reserves the right to examine all information stored on any network device or computer belonging to CCH.
   3. Employees are responsible for exercising good judgment to determine reasonable and proper personal use. If there is any uncertainty, employees should consult their supervisor or manager.
   4. As necessary for security and network maintenance, authorized individuals may monitor equipment, systems and network traffic at any time.
   5. To ensure compliance with this policy, CCH reserves the right to periodically audit networks, systems, messages and other forms of information created, received, transmitted or stored using company electronic media systems.
   6. The electronic media system hardware and software is the property of CCH.
   7. Occasional or incidental use of electronic media for personal, non-business purposes is considered acceptable, provided: 1) such use does not violate any law or regulation; and 2) does not substantially diminish job performance and productivity.
   8. Every information security related asset shall be assigned to an owner. The owner will be responsible for determining acceptable use, and for implementing all applicable CCH policies, procedures and controls.
   9. Review of the policies for information security every 2 years or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
   10. CCH must identify all legal, regulatory and contractual requirements.

B. Confidentiality
   1. All information composed, sent or received via CCH systems is considered the property of CCH. This information is not the private property of any employee.

2. Employees should not assume electronic media communications will be kept private and confidential. Even when a message is erased, it is still possible to retrieve and read the message.
3. Employees must recognize that all forms of electronic media may be used as evidence in legal cases.
4. E-mail sent via the Internet is normally transmitted unencrypted and therefore not secure. Such e-mail is easily read if intercepted or compromised. Never include any information that you intend to keep private and confidential in an email message.
5. Messages sent with confidential files or material must have appropriate security measures built in, such as the use of passwords or encryption techniques.
6. Any personnel applying encryption to CCH-owned electronic media must, upon the request of management, provide the keys or passwords needed to decrypt such media.

C. Resource Handling

1. Employees must safeguard the physical security of all offsite equipment entrusted to them, whether attended or unattended.
2. Appropriate care and diligence is required when traveling with equipment, e.g. laptops, Internet broadband cards and smartphones.
3. Laptops must be kept close to the employee while traveling. Do not leave laptops unsecured in personal vehicles, rented vehicles or unattended in common areas such as airports, hotel lobbies or other sites.
4. Employees shall not lend any mobile device or broadband access card to anyone without overseeing its use.
5. CCH may, at its discretion and for valid business purposes, provide wireless network access for approved portable devices. Use of the wireless network for personal reasons should be avoided, particularly regarding applications with high bandwidth demands, such as audio or video streaming or very large file downloads.
6. Production systems equipment (server and network), information, or software shall not be taken off-site without prior authorization.

D. Email

1. All messages sent by electronic mail are official records. CCH reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose.
2. Management may review all electronic mail communications to determine whether such messages may have breached security, violated CCH policy, or taken other unauthorized actions.
3. CCH may also disclose electronic mail messages, as required by law, to law enforcement officials without notice to, or the explicit consent of, the workers who may have sent or received such messages.
4. Any personal use of e-mail must not interrupt or jeopardize normal business activities. Personal e-mail must not be used for solicitation, to support for-profit outside business activity, or harm CCH's reputation and goodwill.
5. Except as authorized by the information owner, personnel must not forward electronic mail containing sensitive information to any address outside the CCH network.
6. Extra care should be taken with recipients of outgoing email. Any email sent to external addresses cannot be recalled. Personnel should review all “To:”, “CC:” and “BCC:” email addresses prior to selecting ‘Send’. Be particularly cautious about the use of the “Reply All” feature.
7. Employees must not send EPHI, credit card numbers, log-in passwords, other security information or payment information via electronic mail if the information is in readable (unencrypted) form. Email encryption must be used when sending sensitive information.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders. If there is any doubt regarding the safety of these attachments, contact IT as soon as possible.
9. Email is a business communication tool and should represent the organization in a consistent, professional manner, and adhere to the same standards as other materials.

a. No decorative and/or colored fonts are to be used in the body of the email and the signature line.
b. Quotations or personal philosophies should not be included in email signatures.
c. No colored or patterned backgrounds or graphics (.gif) should be used unless approved CCH logos. Approved logos are those that conform to the CCH graphic and communication standards.

Note: The following is an example of an appropriate email signature:
James Smith (full name in bold), Project Coordinator (Job Title)
Employee Relations (Department)
Campbell County Health (Organization)
307.688.1234 (Desk or dept. telephone number, fax, 800)
James.smith@cchwyo.org (Email address) www.cchwyo.org (Website address)
Disclaimer is automatically included on all outgoing CCH email messages.

10. The following activities are strictly prohibited, with no exception:
    a. Using the email system to send or forward pornographic material.
    b. Using the email system for any form of harassment whether through language, content, frequency or size of message.
    c. Sending unsolicited bulk email messages, including the sending of "junk mail" or other advertising materials to individuals who did not specifically request such material (email spam).
    d. Sending or forwarding emails of a non-business nature to the "All Employee" list.
    e. Creating or forwarding "chain letters", "Ponzi" schemes or other get rich quick "pyramid" schemes of any type.
    f. Using the E-mail system in a manner that would violate the CCH Information Security Policy.

E. Internet and Social Networking Use
1. When using the Internet, the laws for copyrights, patents, and trademarks must be respected.
2. The IT department may prevent users from connecting to certain non-business web sites. Whether intended or accidental, workers who discover they have connected to a web site containing sexually explicit, racist, other potentially offensive material, online gambling, unauthorized download services, or software piracy download sites (e.g. bit-torrent based), must immediately disconnect from that site. The ability to connect to a specific web site does not by itself imply that users of CCH systems are permitted to visit that site.
3. All files downloaded from non-CCH sources via the Internet (or any other public network) must be screened with malware detection software. This screening must take place before the file is opened or examined via another program.
4. Users must not place confidential or internal CCH material (software, internal memos, press releases, etc.) on any publicly accessible Internet computer system without obtaining the explicit consent of management.
5. Postings by employees from a CCH email address to newsgroups or other social networking sites, unless such posting is during business duties, is strictly prohibited.
6. The following activities are strictly prohibited, with no exception:
    a. The intentional viewing of pornographic material.
    b. Online gambling. This includes real time gambling sites as well as other sites that allow for the ability to place domestic or "off shore" wagers.
    c. Malicious uploading or downloading personal or company information from any Internet based Personal Network Storage and Backup Sites. Examples would be Dropbox.com, Google Drive, OneDrive.com, Box.net, or other cloud storage sites.
    d. Online gaming. This includes live interactive games, Peer-to-Peer games, or games that are based off websites outside of our network.
    e. Selling or purchasing personal items via online auction sites, for personal use. (examples: Ebay, Yahoo Auction, Craigslist).

f. Accessing any external email system for non-business-related purpose via the internet, SMTP, POP3, IMAP or other protocol. This includes web-based systems like GMail, Hotmail, Yahoo Mail, and others.
g. Accessing outside websites for the purpose of "job hunting" outside of the organization. This would include other employer's websites or websites that provide you the ability to post your resume for other employers to view.
h. Port scanning, network probing or security scanning.
i. Accessing any website that allows access to Peer-to-Peer network sharing of music files, movies, programs, or other information.
j. Listening to or viewing, for any non-business-related activity, any live or real time Streaming media files. Examples would be web-based radio or music stations or web-based TV stations.
k. Downloading or installing any unauthorized programs or files from the internet.
l. Accessing any public Instant Messaging or Chat service for non-business related activity. Some examples would be MSN, Yahoo, IRC.
m. Updating or maintaining a personal website or Blog site.
n. Accessing "Online Dating" (Examples: Match.com, eharmony.com, etc.) websites.

7. The following activities are limited to business use only:
   a. All social networking sites such as Facebook and Twitter.
   b. Portable Music devices or MP3 players. Examples: Ipods, Zunes, etc.
   c. Digital Cameras; Any type of USB memory or mass storage device.
   d. Any type of wireless network equipment.

8. Other Unacceptable Use
   a. It is unacceptable to violate the rights of any person or company in respect to copyright, trade secret, patent or the use of other property protected under similar laws or regulations. Violations may include, but are not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CCH.
   b. The unauthorized distribution of copyrighted material including, but not limited to, copyrighted music or the digitization and distribution of photographs from magazines, books or other copyrighted sources, is unacceptable.
   c. The introduction of malicious software programs (e.g., viruses, worms, Trojan horses, e-mailbombs, etc.) into the production network or into any information processing device is unacceptable.
   d. Revealing your active directory account password to others or allowing use of your account by others is unacceptable. Examples include writing down a personal password then posting that password either on your computer equipment and/or in the workspace.
   e. It is unacceptable to use a CCH computing asset to actively engage in procuring or transmitting pornographic material or similar objects in violation of existing sexual harassment or hostile workplace policies.
   f. It is unacceptable to send fraudulent offers of products, items, or services from any CCH account.
   g. Maliciously breaching security or disrupting production network communication is unacceptable. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
   h. Port scanners, packet sniffers or other diagnostic and testing tools are expressly prohibited on production resources unless the VP-IT is notified in advance and approves such use. However, when these analysis tools are used as part of an authorized employee's ordinary duties, no separate approval is needed.
   i. It is unacceptable to execute any form of production network monitoring which will intercept data not expressly addressed to and intended for the recipient, unless this activity is a part of the employee's normal job responsibilities.

j. Circumventing user authentication or security measures on any production host, network or account is unacceptable, unless it's a job requirement, is temporary, and authorized by IT.

k. Personnel shall not provide information about patients to unauthorized external entities without explicit senior management and patient approval.

l. It is unacceptable to send unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). any form of harassment via email, telephone or paging, whether through inappropriate language or pictures, frequency, or size of messages, is prohibited.

m. Unauthorized or non-business use of provided video conferencing facilities or webcams is unacceptable. Video devices must never to be used to access adult-based websites.

ENFORCEMENT:

Violation of any CCH Information Security policy may result in disciplinary action, up to and including termination of employment or contract.

REFERENCES:

- Disciplinary Actions CCH Human Resources policy

INITIATED BY: Matt Sabus, VP of Information Technology DATE: May 7, 2020
REVIEWED BY: Travis Leonard, Manager, IT Infrastructure DATE: May 14, 2020
APPROVED BY: Mary Lou Tate, CFO DATE: July 22, 2020

Policy Committee Approval History

Version	Date	Description	Approved By
1.0	8/11/2020	Initial policy release	Leadership Council