# CLAIBORNE COUNTY HUMAN RESOURCE AGENCY/ PUBLIC TRANSPORTATION

# TECHNOLOGY POLICY

# Table of Contents

# Claiborne County Human Resource Agency/Public Transit
# Technology Policy
# Effective: November 1, 2016
# Revised: May 14, 2021

The vision of Claiborne County Human Resource Agency/Public Transit (CCHRA) includes a call to embrace "today's technology." This policy exists to further that vision and ensure all members of the CCHRA community have the information technology tools, training, and support they need to be successful.

## I. Information Systems Virus Management Policy & Procedures

### Purpose

This policy and procedures document describes the responsibilities and steps necessary to keep CCHRA's network and computers safe from virus attacks and other malware.

### Scope

This policy applies to all workstations, laptops and servers that are connected to CCHRA's network and to any end-user that is using a device connected to the network.

### IT Personnel Responsibilities

The IT Personnel is responsible for:

- The Ensuring virus protection is installed and configured on all agency workstations, laptops and servers
- Maintaining an automatic virus protection system, currently McAfee's Policy Orchestrator, that pushes updates and upgrades to workstations at least weekly and to servers at least daily with limited end-user interaction
- Removing any infected device from the network until the virus has been cleaned
- Keeping copies of virus-detection and eradication tools offline
- Educating end-users of the danger of opening emailed file attachments they were not expecting to receive

## End-user Responsibilities

The end-user at CCHRA, including office staff, drivers, and any individual who has a device that connects to CCHRA's network, is responsible for following the best practices listed in this policy.

### Best Practices

- Always run the virus protection software that is loaded on the desktop. (CCHRA uses McAfee's anti-virus solution.) If anti-virus software is not loaded on the computer, download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying the Trash.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is an absolute business requirement to do so.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- New viruses are discovered almost every day. Periodically check the anti-virus software's status to confirm the computer is being protected and is updating properly.

## II. Laptop, Tablets and Mobile Device Use Policy

### Purpose

This policy addresses actions to safeguard information and to minimize risk of loss or theft of CCHRA laptops, tablets or mobile devices and/or data and the associated impact on CCHRA

### Scope

This policy applies to all employees, contractors, and any CCHRA personnel who use or are responsible for a CCHRA-supplied mobile device, or storage medium that contains CCHRA data.

**Use Policy**

1. Protection of the device:
    - Do not leave the device in any vehicle in plain view;
    - Do not leave the device or the case containing the device unattended;
    - Monitor the device carefully when going through security at airports or any public place;
    - Do not allow the device to be serviced or sent to Surplus Property without It consultation; and
    - If the device is lost or stolen, report it immediately to the Executive Director.

2. Data storage on the device:
    - Do not store confidential data on the device;
    - Do not store information about employees or vendors on the local drive/device. Do not store on the device:
        a. Protected health information (HIPAA);
        b. Financial information that could be used against clients or employees (Social Security numbers, credit card numbers, bank or financial account numbers, mother's maiden name, for example;) and/or
        c. Any other sensitive information.
    - Do not store full data sets (full database copies or extracts) on the device;
    - Do not store other files or email on the local drive/device that may contain any of the above protected or confidential information; and
    - If local storage of confidential data on the device is unavoidable, contact the Executive Director and IT Personnel.

3. A mobile device as used herein is defined as any electrical and/or battery-operated device that can be easily transported and that has the capability for storing, processing, and/or receiving/transmitting data including Smartphones, Blackberrys, Tablet/Mini PCs, PDAs, and Hand-Held PCs. Mobile devices (either CCHRA-owned or employee-owned) used to access CCHRA systems (including email) or for storage of CCHRA data must be appropriately secured to prevent sensitive data from being lost or compromised, to reduce the risk of spreading viruses/malware, and to mitigate other forms of abuse.

4. The physical security of any of these devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. When stored, devices shall be

stored in a secure place, preferably out-of-sight.

5. To protect against potential loss of CCHRA information assets, data files on the mobile device or removable cards should be backed up to a secure location on the CCHRA internal network. Mobile device users must minimize the potential loss of data via Wi-Fi, cellular, or Bluetooth connections to their device by configuring the device in a secure manner or turning those services OFF when not in use.

6. Device users must enable screen locking and screen timeout functions on all mobile devices.

## Cell Phone/Hand Held Device Use Policy

Our Company recognizes that the employees are our most valuable asset, and the most important contributors to our continued growth and success. Our company is firmly committed to the safety of our employees. CLAIBOREN COUNTY HUMAN RESOURCE will do everything possible to prevent workplace accidents and is committed to providing a safe working environment for all employees.

To further this goal, CLAIBORNE COUNTY HUMAN RESOURCE has developed a Cell Phone/Hand Held Device Use Policy effective 05.

**Purpose:**

Driver inattention is a factor in a majority of motor vehicle accidents. We are not only concerned about your welfare as a CLAIBORNE COUNTY HUMAN RESOURCE EMPLOYEE, but also the welfare of others who could be put in harm's way by inattentive driving. Mobile phones and other hand held device use while driving is a common, often harmful, distraction. Many countries and localities have prohibited mobile phone/hand held device use while driving. Researchers at the University of Toronto found the risk of having a traffic accident while using a cell phone or similar device to be the same as driving drunk. For these reasons, drivers may not use hand held devices to place work-related calls or while operating a vehicle while on company business.

As a driver, your first responsibility is to pay attention to the road. When driving on CLAIBORNE COUNTY HUMAN RESOURCE business or driving while conducting business on behalf of the company in any other manner, the following applies:

**Procedures:**

Definition – Mobile Hand Held Units: Hand held devices may include cell phones, pages, palm pilots, faxes and other communication devices.

- Allow voicemail to handle your calls and return them when safe
- If you need to place or receive a call, pull off the road to a safe location and stop the vehicle before using your phone.
- Ask a passenger to make or take the call.
- Inform regular callers of the best time to reach you based upon your driving schedule.
- The only exception to this police is for calls placed to 9-1-1.
- If placing or accepting an emergency call, keep the call short and use hands-free options, if available.
- When receiving an emergency call, ask the caller to hold briefly until you can safely pull your vehicle off the road

## III. Video Surveillance Review

**Purpose**

This policy addresses actions randomly and consistently reviewing surveillance camera data on employees and clients' behavior of those who are aboard CCHRA's vehicles or any other property and associated impact on CCHRA

**Scope**

This policy applies to all employees, contractors, and any CCHRA personnel who are on or utilize any of CCHRA's vehicles or property.

**Use Policy**

1. The CCHRA makes limited use of video surveillance systems on its vehicles and office location. Video surveillance systems are primarily used to record access building and vehicle entrances and interior of vehicles and lobbying areas of office location. Video surveillance cameras are also used to provide surveillance of the exterior of the building and surrounding streets.

2. Video surveillance cameras are generally not used to observe employee work areas except the drivers while on vehicles, and are never used in areas where employees would have an expectation, such as restrooms.

3. The primary purpose of the video surveillance system is to allow the after-the-fact investigation of crimes committed against the company or allegations from clients against the agency and/or driver. The system may also be used to assist in the investigation of certain types of occupational health and safety violations.

4. The video surveillance system is not intended to be used as a method of tracking the work habits or productivity of individual employees.

**Management of Video Surveillance Systems**

The CCHRA's IT Department is responsible for the management of all video surveillance systems used at the agency. Other departments shall not install video surveillance system without the knowledge and approval of the Executive Director or IT Department.

**Video Surveillance Monitoring**

The video surveillance systems are capable of being monitored from the IT's Desk located at the 1703 Bridewell Lane. IT Personnel generally view video surveillance cameras on a periodic basis or in response to a specific incident. Because of the many responsibilities of the IT Personnel, the video surveillance system is not monitored on a continuous basis.

**Video Surveillance Recording**

1. All video surveillance cameras are capable of being recorded continuously by a digital video recording system, Recorded video is used exclusively for the investigation of security and safety incidents and not for other purposes.

2. The CCHRA's IT Department is responsible for the management of the video surveillance system and has exclusive control of the release of video recordings produced by this system. Recorded video is not made directly available to CCHRA's employees, clients, or the general public, in the event that an incident occurs, employees should report the incident to the Executive Director or Operation Supervisor who will then report to the IT Department. If the event occurred in an area where video surveillance coverage is available, the IT Personnel will review the recorded video and report to Executive Director to make a determination if any video relevant to the incident is available. This video will be used by the Executive Director to investigate and resolve the reported incident.

3. Requests to provide video recordings directly to non-employees (such as clients or members of the general public) will not be accommodated. If an incident has

occurred, non- employees should be encouraged to report it to the Executive Director. If it is believed that recorded video from the CCHRA would assist in the investigation of the incident, the police/lawyer should be told to contact the Executive Director of CCHRA. If relevant video is available, a permanent video clip of the incident will be produced and made available to the police/lawyer. All requests for video recordings by law enforcement agencies shall be coordinated through the CCHRA's Executive Director.

4. Recorded video is generally stored for a period of thirty days. Any video associated with a specific incident or event is generally converted into a permanent video clip and stored for the duration of the investigation. Video clips which could become evidence in civil or criminal proceedings are kept indefinitely unless other direction is given by the Legal Department.

**Limitations of Video Surveillance Systems**

**1.** Employees should be aware that an IT Personnel is not watching most cameras most of the time and 1 employees should not have an expectation that they are under continuous surveillance when they are in the range of a camera. Employees should also be aware that the video surveillance system has cameras that cover only a small fraction of the total campus and vehicles, and even when camera coverage exists, it may not provide the level of detail necessary to spot suspicious activity or identify criminals.

## IV. Social Networking Policy

**Purpose**

The purpose of this policy is to ensure that the company's employees understand their obligations when using social media, such as Facebook, twitter, blogs, and are informed of the importance of managing the risks associated with such use that may impact on the reputation of the company and/or the safety of its employees and that may result in a breach of the company's Conduct of Conduct and, policies, procedures or instructions. This policy is for the mutual protection of the company and its employees and is not intended to prevent, discourage or unduly limit employees' expression of personal opinion or online activities.

**Scope**

This policy applies to all employees and contractors of CCHRA.

At CCHRA, we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media.

## 1. Guidelines

In the rapidly expanding world of electronic communication, *social media* can mean many things. *Social media* includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with CCHRA, as well as any other form of electronic communication.

The same principles and guidelines found in CCHRA's policies and three basic beliefs apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow associates or otherwise adversely affects members, customers, suppliers, people who work on behalf of CCHRA or CCHRA's legitimate business interests may result in disciplinary action up to and including termination.

## 2. Know and follow the rules

Carefully read these guidelines, the CCHRA's Statement of Ethics Policy, the CCHRA's Information Policy and the Discrimination & Harassment Prevention Policy, and ensure your postings are consistent with these policies. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

## 3. Be respectful

Always be fair and courteous to fellow associates, customers, members, suppliers or people who work on behalf of CCHRA. Also, keep in mind that you are more likely to resolved work-related complaints by speaking directly with your co-workers or by utilizing our Open Door Policy than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, members, associates or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or

posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy.

**4. Be honest and accurate**

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about CCHRA, fellow associates, members, customers, suppliers, people working on behalf of CCHRA or competitors.

**5. Post only appropriate and respectful content**

- Maintain the confidentiality of CCHRA's trade secrets and private or confidential information. Trades secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential communications.
- Respect financial disclosure laws. It is illegal to communicate or give a "tip" on inside information to others so that they may buy or sell stocks or securities. Such online conduct may also violate the Insider Trading Policy.
- Do not create a link from your blog, website or other social networking site to a CCHRA website without identifying yourself as a CCHRA's associate.
- Express only your personal opinions. Never represent yourself as a spokesperson for CCHRA. If CCHRA is a subject of the content you are creating, be clear and open about the fact that you are an associate and make it clear that your views do not represent those of CCHRA, fellow associates, members, customers, suppliers or people working on behalf of CCHRA. If you do publish a blog or post online related to the work you do or subjects associated with CCHRA, make it clear that you are not speaking on behalf of CCHRA. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of CCHRA."

**6. Using social media at work**

Refrain from using social media while on work time or on equipment we provide, unless it is work-related as authorized by your manager or consistent with the Company Equipment Policy. Do not use CCHRA's email addresses to register on social networks, blogs or other online tools utilized for personal use.

**7. Retaliation is prohibited**

CCHRA prohibits taking negative action against any associate for reporting a possible deviation from this policy or for cooperating in an investigation. Any associate who retaliates against another associate for reporting a possible deviation

from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

## 8. Media contacts

Associates should not speak to the media on CCHRA's behalf without contacting the CCHRA Board of Directors or Executive Director. All media inquiries should be directed to them.