

Delta Community Action Foundation, Inc.

Acceptable Use Policy and Technology Agreement

It is our goal to provide technological assistance to each facility, to accommodate staff members, and to reduce paperwork. It has taken us a long time to acquire this equipment. Therefore, the maintenance and upkeep of this equipment is paramount to ensuring everyone can have the tools needed to do their job. It is imperative that each staff member follows the regulations set forth in the contract. The policies and regulations listed below apply to all programs under Delta Community Action.

CONFIDENTIALITY IS TO BE MAINTAINED AT ALL TIMES

- We have installed video and audio surveillance cameras at some of our centers for security and safety purposes. Audio and video monitoring is being conducted.
- Employees are responsible for the reasonable care and security of the computer system components that they are assigned for use. Employees will promptly report the damage, destruction, or theft of any hardware.
- Employees may be subject to discipline and held financially responsible for any equipment that is lost, stolen, or damaged because of the employee's negligence, misuse, or abuse.
- Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. All activity on devices connected to the network may be monitored, intercepted, recorded, copied, audited, inspected, and disclosed to authorized personnel and law enforcement without prior notice. Unauthorized or improper use of this system may result in disciplinary action, and civil or criminal penalties.
- Users must comply with all applicable laws and regulations regarding computer and internet access, such as the Children's Internet Protection Act (CIPA).
- Work email addresses, usernames, and passwords will be assigned to employees. Each user is responsible for keeping their passwords confidential. Please do not share sensitive credentials with anyone other than the IT Specialist. All computers will have a secure login. **DO NOT** change computer logins and passwords without prior approval from the IT Specialist.
- Never give your passwords to anyone else, with the exception of the IT Specialist. Please reach out to the IT Specialist if you have any problems accessing ChildPlus, Teaching Strategies, or your deltacaf email address.
- Employees are responsible for any actions taken while logged in using their user ID.
- Users should not delete, exam, copy, or modify files and/or data belonging to other users without prior consent.
- Users are prohibited from visiting sites that contain gambling, pornography, or other obscene material.
- Users are prohibited from illegal sharing of copyrighted materials. More information regarding copyright law can be found at <https://www.copyright.gov>
- Computers are to be used for work and school related activities; not for personal use

- Email is provided for work and school use only. Forwarding chain letters, jokes, memes, hyperlinks, and other junk mail is prohibited. These types of emails are a common way of transmitting viruses and other malicious content.
- Do not store personal pictures, videos, music, or other personal files on computers. Unnecessary files are periodically deleted.
- No personal printing
- Volume printing is prohibited at centers. Please email documents to be printed on one of our bulk printers. If you have any questions, please contact the IT Specialist.
- A signature is required to check out computers. Any equipment that is checked out should be returned in a timely manner in the same condition that it was issued.
- It is all staff members' responsibility to educate students about appropriate online behavior, including interactions with other individuals on social networking sites/chat rooms, and cyber bullying awareness and response.
- Internet traffic will be filtered to prevent access to obscenity, child pornography, and other materials harmful to minors.
- I will not give out confidential information to anyone via the Internet that could be used to identify myself, others, or students. This includes, but is not limited to, addresses, phone numbers, school locations, or other personally identifiable information.

If you are unsure of what you are doing, please stop and call the IT Specialist.

Social Media

- Do not post information online that is confidential and proprietary to Delta Community Action, or any of its programs.
- Do not post material that is threatening, harassing, illegal, obscene, defamatory, slanderous, or hostile towards any individual or entity.
- Do not promote or advertise a commercial product or solicit business or membership or financial or other support in any business, group, or organization for personal gain.

Please note that social media is part of the internet. Some examples of social media include Facebook, Snapchat, Instagram, YouTube, Twitter, Reddit, Pinterest, and TikTok.

As an employee of Delta Community Action, and any program under Delta Community Action, I have read and understand the policies above. I agree to abide by all rules and regulations set forth by Delta Community Action. I also understand that violation of these can result in disciplinary action.

Employee (Printed): _____ Date: _____

Employee Signature: _____ Date: _____