



ANDERSON COUNTY
SHERIFF'S OFFICE

GO - 234

GENERAL ORDERS

COMPUTER SYSTEMS, ELECTRONIC MEDIA AND OTHER ELECTRONIC SYSTEMS

PURPOSE:

Efficient, effective and secure communication is essential to the operation of the Sheriff's Office and the County of Anderson. The purpose of this policy is to establish and provide guidelines in the proper use of electronic equipment, systems, tools and resources provided to employees by the County of Anderson, the Sheriff's Office, SLED, NCIC, CJICS or other sub-systems and approved service providers.

POLICY:

Resources available to employees from all computer and electronic informational systems or electronic media are to be used to further the goals and objectives of the Sheriff's Office and the County of Anderson by providing an effective method to:

- Communicate
- Perform research
- Obtain information while performing law enforcement related tasks

Employees are expected to use good judgment while using any and all computer related resources and electronic media. Employees are to abide by the following:

- All software licensing agreements and restrictions
- User agreements between the employee and this office or the employee and other departments within Anderson County
- Requirements set forth by SLED, NCIC and CJICS
- All applicable security requirements set forth by this Office, the County of Anderson, State and Federal Agencies, or other sub-systems and approved service providers

PRIVACY:

Electronic media, specifically the Internet and e-mail, is not a secured communication network, and others can potentially read personal or privileged information via these media.

Employees have no expectation of privacy:

1. In sending or receiving electronic messages and information on the Internet
2. With computer workstations, equipment, hardware and software owned by this office or the County of Anderson

NOTE: *This Office reserves the right to monitor, inspect and audit all electronic messages and information received, sent or distributed through any computer system owned by this Office and the County of Anderson, or accessed by our computer system.*

INTERNET:

The Internet is a legitimate law enforcement resource and investigative tool. Sheriff's Office users are to adhere to the following when accessing the Internet:

- Use of the Internet is for legitimate law enforcement purposes only.
- Internet game playing is prohibited.
- The Internet is not to be used in any manner deemed inappropriate.
- Accessing offensive and inappropriate websites is prohibited unless a legitimate law enforcement need exists and only with prior supervisory notification and subsequent approval.

NOTE: *Due to the need to access certain websites for legitimate research purposes, the Criminal Investigation Division's Vice & Narcotics units are permitted unrestricted access to websites that would otherwise be considered offensive and inappropriate.*

**E-MAIL AND
MESSAGING
SYSTEMS:**

E-mail and messaging systems are valuable tools that can enhance the effectiveness and efficiency of the Sheriff's Office. Employees are to adhere to the following guidelines for e-mail / messaging use:

- The e-mail and messaging system is to be used for business purposes only.
- There is no expectation of privacy between e-mail or messaging system users.
- The e-mail and messaging system is subject to routine monitoring.
- Use of inappropriate or offensive language is prohibited.
- All e-mail and messaging system text is subject to public review via the Freedom of Information Act.

NCIC USAGE:

The Anderson County Sheriff's Office is responsible for security of SLED/CJICS/FBI files within our agency. Guidelines are in place to enhance security of the use of these files. Each certified operator is responsible for insuring this policy is adhered to at all time through the use of SLED functions by interface systems and the SLED terminals which have a direct line to SLED.

The direct connection to SLED is protected by internal firewalls between the ACSO computer network, the NCIC file server and the dedicated router to SLED. The South Carolina state CIO's office sets-up the dedicated router and regulates the NCIC software. SLED contracts with a third-party who installs the hardware and performs the initial software set-up. No ACSO employees are involved in this process.

Data stored in NCIC is documented criminal justice information, and must be protected to ensure correct, legal, and efficient dissemination and use. The individual receiving a request for criminal justice information must

ensure the person requesting the information is authorized to receive the data. The stored data in NCIC is sensitive and should be treated accordingly.

An unauthorized request or receipt of NCIC material could result in criminal proceedings or interdepartmental disciplinary action of any infraction of the misuse of the system. This policy includes correct documentation for entry purposes as well as inquiries.

All NCIC/SLED/CJICS/DMV systems are to be used for law enforcement purposes only and should not be disseminated to the public.

SECURITY PROTOCOL: **An annual audit** will be conducted of the central records computer system for verification of all passwords, access codes, or access violations.

Outside computer software will be introduced into the central computer system only with the approval of the system administrator and after necessary precautions have been taken to ensure that there is no threat of contamination.

All computer files will be backed up according to a regular schedule. A complete backup will be performed every 24 hours and the archival tape storing this information will be stored off-site as needed.

**WIRELESS ACCESS
PROCEDURES:**

Wireless access points within Anderson County are available for use by ACSO deputies. When parked at these locations, deputies have secure access to the agency's **PD-Manager™** System. (See Appendix for locations.)

The following procedures should be followed to properly access the system:

1. Drive up to the Wireless Access Point.
2. Boot the laptop computer.
3. Verify on-line connectivity is available. A green bar in the lower right corner of the display screen indicates a proper connection.
4. Login to the County Network using the assigned user-code and password.
5. Login to **PD-Manager™**. (See the **PD-Manager™** User's Guide for user information.)

Deputies are authorized to keep an assigned laptop until the end of their duty rotation, at which time laptops and in-car chargers should be returned to the Roll Call room. It is the responsibility of the deputy returning the equipment to plug the laptop into an available charger.

NOTE: *If connectivity is unavailable at a particular wireless site, a supervisor should be notified. Shift supervisors are responsible for notifying Information Technology.*

**UNAUTHORIZED USE OF
COMPUTER, ELECTRONIC,
AND INFORMATION
SYSTEMS:****Violations include, but are not limited to, the following:**

- No one shall use any computer, computer system or network facility without proper authorization.
- No one shall assist in, encourage, or conceal from this Office or other authorities any unauthorized use, or attempt unauthorized use, of any computer, computer system or network facility.
- No one shall knowingly endanger the security of any computer, computer system or network facility nor willfully interfere with others authorized for usage of these systems.
- No one shall give away or share any password assigned to them to access any computer, computer system or network facility without proper authorization.
- No one without specific authorization shall read, alter, or delete any other person's computer files or electronic mail.
- Transmitting any material or messages in violation of Federal, State, local law or County policy, including sexually, racially, or ethnically offensive comments, jokes, slurs, threats, harassment, slanders, or defamation
- Accessing or distributing obscene or suggestive images or offensive graphical images
- Distributing sensitive or confidential information
- Distributing unauthorized broadcast messages or solicitations
- Using County provided electronic media to accomplish personal gain or to manage a business
- Distributing copyrighted materials not owned by the County, including software, photographs, or any other media
- Downloading of copyrighted information or software
- Developing or distributing programs designed to infiltrate computer systems internally or externally
- Accessing or downloading any resource for which there is a fee without prior, appropriate approval
- Attempting to access any system an employee is not authorized to access (hacking)

- Listening to voice mail or reading electronic mail of another employee without prior, written approval of the Sheriff
- Political endorsements

**DISCIPLINARY
ACTION:**

Violations of this policy will result in disciplinary action appropriate to the violation. **Disciplinary action** may include one or more of the following:

- Counseling
- Written reprimand
- Suspension from duty without pay
- Termination of employment
- Criminal prosecution

Approved by:
John S. Skipper, Jr., Sheriff

APPENDIX
Wireless Access Points**Anderson – 1**

Wren High School – Front student parking lot, front drive
Palmetto Middle School – Back of building on side facing football stadium parking lot
Powdersville Middle School – Back parking lot

Anderson – 2

Belton Middle School – Side parking lot (works beside road if gate is locked)
Honea Path Middle School – Back parking lot beside dumpsters

Anderson – 3

Starr Elementary School – Front of building
Iva Elementary School – Front of building

Anderson – 4

Pendleton High School – Front of building
Townville Elementary School – Front parking lot

Anderson – 5

TL Hanna High School – Front of building
Westside High School – Front of building
South Fant Elementary – Front side of building