

Directive	Computers and Records	800-1	1 of 14
Effective Date	January 1, 2010		



Wilkesboro Police Department

Electronic Written Directives Document

I. PURPOSE

The purpose of this directive is to provide procedures and guidelines for the collection, storage and dissemination of records within the Wilkesboro Police Department.

II. POLICY

The Wilkesboro Police Department shall establish control procedures to meet the management, operational and informational needs of the department in the collection, security, dissemination, retention and disposition of records. The Records Section will coordinate the administration, field reporting and central records functions of the department.

III. DEFINITIONS

- A. Division of Criminal Information (DCI): The component of North Carolina state government that collects and disseminates statewide crime data
- B. Incident-BASE Reporting (IBASE): North Carolina Incident Base Reporting System that Wilkesboro Police Department uses to submit crime data to the State of North Carolina and the Federal Bureau of Investigation for UCR.
- C. National Crime Information Center (NCIC): A federal agency that collects and disseminates nationwide crime data through local agency submission
- D. Records Management System (RMS): The Department's computerized system for central records management.
- E. Uniform Crime Reporting (UCR): A systematic crime reporting program that results in local, state, and national crime statistics.

IV. ACCESS AND SECURITY OF RECORDS

- A. The Administrative Assistant shall be responsible for the security of the Department Records Area. All entry doors leading to the Records Section will be kept secured except during business hours when doors to Records may remain open as long as staff personnel are available to monitor access.

Directive	Computers and Records	800-1	2 of 14
Effective Date	January 1, 2010		

- B. Reports shall be placed in file cabinets located in a lockable room. This room shall always be maintained by an authorized police employee during business hours and then after hours the room shall be locked. Supervisors shall have continuous access to the file cabinets; patrol and investigations may access the files with supervisor permission. Department records, which include Incidents, Arrests, Warrants, Citations, and Traffic Accidents, are available to all sworn personnel through RMS with password-protected access.
- C. Officers needing reports shall make a request to the Administrative Assistant in writing, which may be in the form of e-mail. The request shall list the:
 - 1. OCA Number of the report, or other identifying information if the OCA is not known;
 - 2. The date requested;
 - 3. If a copy or the original is needed;
 - 4. The reason for the request;
- D. The Administrative Assistant will retrieve the record from the files and provide either the original or a copy. If the officer needs the original, the Administrative Assistant will retain the request submitted by the officer to document the location of the report. When the report is returned, the Administrative Assistant will return the request to the officer.
- E. 24-hour access to Department Records and Reports is provided to officers through the computerized Records Management System (Police Pac).
- F. Access to the Police Pac is password controlled. The system administrator for the Wilkesboro Police Department computer network must grant new employees access to the network and to authorized applications including Police Pac.
- G. Information shall be released to the media and public in accordance with public records law and governing policy covered in Public Information.

V. JUVENILE RECORDS

- A. All Juvenile Criminal reports are turned into Records and are filed daily in a separate locked drawer. These reports are not public record and are not filed with other reports.
- B. Fingerprints and photographs of juveniles taken pursuant to NCGS 7B-2102

Directive	Computers and Records	800-1	4 of 14
Effective Date	January 1, 2010		

d. Accident Form DMV-349

3. Whenever filling out a field report, officers should refer to the Incident Based Crime Reporting manual located in the Records Section.
4. Officers should follow the procedures outlined in the Incident Base Crime Reporting manual.
5. Field (incident) reports shall be submitted by the officer before the end of tour of duty, to be read and approved. The supervisor (or acting supervisor) shall read, approve all reports submitted. Reports are then submitted through the automated records management to the Division Commander for final approval. Once the reports are approved they will be forwarded to the Records Section for storage and dissemination to appropriate Division or Section.

B. Reporting of Incidents

1. Reports are required to be written for every incident in one or more of the following categories if the incident is alleged to have occurred in this agency's service area:
 - a. citizen reports of crimes
 - b. citizen complaints
 - c. incidents resulting in an employee being dispatched or assigned
 - d. criminal and non-criminal cases initiated by law enforcement employees
 - e. incidents involving arrests, citations, or summonses

C. Case Numbers

Case numbers are automatically generated through Central Communication's CAD system in chronological order. Each case has a unique number.

D. Review of Reports

Supervisors or his/her designee will read and approve each report written. The report will then be electronically approved by the supervisor or his/her designee.

Directive	Computers and Records	800-1	5 of 14
Effective Date	January 1, 2010		

E. Distribution of Reports and Records

Specialized reports are distributed to appropriate Law Enforcement personnel by the Deputy Chief. No reports are distributed outside the agency unless the crime/incident committed is found to have occurred outside the agency's service area, after the report was taken.

F. Index Files

Incidents by type, location and property, whether stolen, found, recovered or seized are maintained through the computer system.

G. The Department participates in the National Incident-Based Reporting System (NIBRS). Crime incident information entered in the Department's Records Management System is used to generate a report containing the statistical data required for Incident-Based Refer to the Visions User Document, Generating IBASE Report Data for instructions on generating the report.

H. The IBASE Report is generated monthly by the Administrative Assistant and electronically submitted by Internet directly to the State Bureau of Investigation, Division of Criminal Information (DCI).

VIII. RECORDS ACCESIBILITY

A. The Records Section of the police department is open 9:00 a.m. until 5:00 p.m., allowing assistance to officers and citizens with requests for hard copies of department records. After hours records information is accessible to all department personnel through the Records Management System.

B. Limited access to certain records is available to officers 24 hours a day/ seven day a week using Rambler, P2P (Police to Police), an internet service connecting Wilkesboro Police Department Records to other law enforcement agencies allowing information to be shared. This service is password protected.

IX. STATUS CONTROL

A. The Investigations Commander will generate a monthly report from the Assigned Cases database showing assigned cases that are open, with the date the most recent follow-up report was submitted, and forward to the assigned investigators. The investigator shall review the open cases report and for cases that have had no report submitted within 30 days, submit supplemental reports within 10 days updating the cases or requesting a status change based on the merits and progress of the investigation

Directive	Computers and Records	800-1	6 of 14
Effective Date	January 1, 2010		

1. If the case has been fully investigated and there are no further leads the case should be closed, leads exhausted;
2. If awaiting results from analysis, an arrest is pending, or there are NCIC entries for the case the status should be listed as inactive.

X. AUDITS

- A. To maintain the integrity of the Records Management System and the security of records contained within the system, the Chief of Police or his designee will complete an annual audit of the Record Management System. This audit will verify all passwords, access codes, and attempt to identify any access violations.
- B. Each time personnel leave the employment of the Wilkesboro Police Department the System Administrator will disable that employees NT Network account and remove all permissions from the Records Management System.

XI. COMPUTERS

- A. The purpose of this section is to ensure protection of the Town's computers, computer systems, and computer networks as well as the data they store and process, and to maintain appropriate operations in a secure, responsible manner. It is critical that these systems and machines be protected from misuse and unauthorized access.
 1. This applies to all Town-owned or leased computer systems and refers to all hardware, data, software and communications networks. Specifically, this includes all computers ranging from multi-user systems to single-user personal computers, computer networks, terminals, printers, modems, wiring/cabling, all software used and any network accessed by these systems including the Internet.
 2. Users are subject to applicable state and federal laws. Improper use or misuse of Town computer systems on a person's work time is a violation of Town personnel policies and may lead to disciplinary action including suspension, demotion or dismissal.
 3. This is not intended to supersede any existing laws or policies regarding records that are confidential. Also, this policy does not address public access issues. It is intended for internal use only.

Directive	Computers and Records	800-1	7 of 14
Effective Date	January 1, 2010		

B. Security

1. Security refers to the protection of all computer equipment resources from any kind of damage and the protection of data from unauthorized access, distribution, modification or destruction. The following procedures will, if used properly, prevent any of the above-mentioned occurrences from happening:
 - a. Users must have authorized access to the Town's computer systems by the Information Technologies Department (IT) and/or Network Administrators (where applicable) after the appropriate department head has requested it in writing. The written request must include the accounts to be accessed by the user. Only the authorized accounts for those systems may be used and only for authorized purposes).
 - b. Users are responsible for safeguarding their own computer access, which includes passwords and logging off when not in use.
 - c. Users SHALL NOT let another person use their access unless IT or Network Administrator (where applicable) approves the use and purpose. Users are directly accountable for all activity connected to their user ID.
 - d. Passwords will be changed every six (6) months and SHALL NOT be divulged to any other person. Passwords should be memorized and not written down unless kept in a secure place.
 - e. Users should log off the system if they must leave the immediate area of their workstation for an extended period of time. (i.e. lunch hours).
 - f. If a user is terminated (for any reason), IT or the Network Administrator (where applicable) is to be notified immediately by the department head so the terminated user can be removed from the system.
 - g. Users SHALL NOT attempt to bypass security mechanisms.
 - h. Users SHALL NOT engage in abuse or misuse of the Town's computing systems as previously defined.
 - i. Users SHALL NOT violate any rules in other portions of the Town Personnel Policy, local, state, or federal laws via Town computing systems or communications.

Directive	Computers and Records	800-1	8 of 14
Effective Date	January 1, 2010		

- j. Users shall disclose to their department head, which shall then notify IT of any suspected or confirmed unauthorized use or misuse of computing systems and also any potential security loopholes.

C. Acceptable Use

1. At all times when an employee is using the Town of Wilkesboro's technology resources, he or she is representing the Town. Use the same good judgment in all resource use that you would use in written correspondence or in determining appropriate conduct.
2. While in the performance of work-related functions, while on the job, or while using publicly owned or publicly provided technology resources, Town of Wilkesboro employees are expected to use them responsibly and professionally. They shall make no intentional use of these resources in an illegal, malicious, inappropriate or obscene manner.
3. The Town understands that a minimal amount of personal use of Town computers and data communications may occur. Personal discretion in the use of those resources must insure that the Town incurs no cost for the use (Town-time or additional charges).
4. The Town of Wilkesboro reserves unto its department heads the right to absolutely curtail such personal use or discretion, as the department head may deem reasonably necessary, on a case-by-case basis.
5. Users are required:
 - a. To respect the privacy of other users; for example, users shall not intentionally seek information on, obtain copies of, or modify files, data, or passwords belonging to other users, unless explicit permission to do so has been obtained. It shall be understood that this rule does not apply to supervisory personnel, who shall have rights to access any files created by users in their departments. All files are Town property.
 - b. To respect the legal protection provided to programs and data by copyright and license. The Town owns licenses to a number of proprietary programs, which allow the Town to use the software, but severely restricts anything other than the use of the software on a single computer or network. Any redistribution of software from the computing systems breaches agreements with our software suppliers, as well as applicable federal copyright, patent and trade secret laws. U.S. Copyright Law provides for civil damages of \$50,000 or more

Directive	Computers and Records	800-1	9 of 14
Effective Date	January 1, 2010		

and criminal penalties including fines and imprisonment in cases involving the illegal reproduction of software. Therefore, no copying, downloading, or distributing of any copyrighted materials, including but not limited to messages, e-mail, text files, program files, image files, database files, sound files and music files is allowed without prior authorization by IT.

- c. To protect data from unauthorized use or disclosure as required by state and federal laws and agency regulations. (i.e. confidential information)
- d. To respect the integrity of computing systems: for example, users shall not use or develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system, or otherwise interfere with data, hardware, or system operation.

D. Unacceptable Use

- 1. Uses that do not conform to the purpose, goals, and mission of the Town and to each user's authorized job duties and responsibilities. Examples of unacceptable activities include but are not limited to:
 - a. Private or personal, for-profit activities (e.g., consulting for pay, sale of goods such as Avon and Amway products, etc.)
 - b. Use for any illegal purpose, including communications that violate any laws or regulations;
 - c. Transmitting or soliciting threatening, obscene, harassing, or politically natured messages or images;
 - d. Viewing pornographic or sexually oriented material, except as deemed necessary to conduct criminal investigations or child-welfare investigations (as approved by supervisor);
 - e. Intentionally seeking information about, obtaining copies of, or modifying of files, other data, or passwords belonging to other users, unless explicit permission to do so has been obtained;
 - f. Interfering with or disrupting users, services, or equipment. Such disruptions would include, but are not limited to:
 - 1). Distribution of unsolicited advertising or messages,

Directive	Computers and Records	800-1	10 of 14
Effective Date	January 1, 2010		

- 2). Propagation of computer worms or viruses and
- 3). Attempting to gain unauthorized entry to another computer or computer system whether owned by the Town of Wilkesboro or outside of the Town.
- g. Removing any computer equipment (hardware, software, data, etc.) without supervisor's authorization and IT notification;
- h. Allowing non-town employees, including an employee's family or friends, to use the Town's technology resources.

E. Electronic Mail

- 1. Electronic mail is intended for Town business only. All e-mail messages are the property of the Town and subject to public inspection. The Town Manager and supervisory personnel have the right to review the contents of employees' e-mail communications.
- 2. When sending or forwarding e-mail, all employees shall identify themselves clearly and accurately including full name, organization, department and full e-mail address. Unacceptable uses of e-mail include, but are not limited to:
 - a. Sending chain letters.
 - b. Sending copies of documents in violation of copyright laws.
 - c. Compromising the integrity of the Town and its business in any way.
 - d. Sending messages containing offensive, abusive, threatening, obscene, harassing, or other language inappropriate for the organization.
 - e. Sending messages that violate the Town's sexual harassment policy.
 - f. Willful propagation of computer viruses.

F. Virus Protection

- 1. Every computer user is to remain alert to the possible transmittal and infection of a computer virus. Most e-mail viruses are transmitted through attachments. Never open attachments that contain the following extensions: .exe, .vbs, .com, .bmt, .hta, .shs, .vbe, .cmd. Upon detecting

Directive	Computers and Records	800-1	11 of 14
Effective Date	January 1, 2010		

any virus, or suspected virus, users are to cease activity immediately and report it to IT or Network Administrator (where applicable).

2. Appropriate anti-viral software will be made available by IT and loaded on every PC or workstation. Users will be expected to update their anti-viral software periodically and instructions will be provided on how to accomplish updates.

G. Internet Use

1. A Town Internet account is a resource granted to employees upon department head approval to increase productivity and provide opportunities for professional growth.
2. All Internet users are expected to comply with Section C (Acceptable Uses) of this Computer & Data Communications Policy. Improper use could result in the cancellation of a user's computer Internet account and will result in disciplinary action.
3. The Internet provides easy access to software distributed by companies on a trial basis. The free access does not necessarily indicate that the software is free or that it may be distributed freely. Users are expected to comply with the copyright policy as previously stated.

H. Compliance

1. The IT Manager and department head will review reported and perceived violations of this policy and may impose restrictions, suspend or terminate computer access, or remove computer equipment during or as a result of an investigation. Other appropriate action in response to abuse or misuse of computer resources may include, but not be limited to:
 - a. Reimbursement to the Town for resources consumed;
 - b. Other legal action, including action to recover damages;
 - c. Disciplinary action, including suspension, demotion, or dismissal pursuant to the Town of Wilkesboro Personnel Policy.
2. Department heads will be responsible for the enforcement of the Town's Computer and Data Communications Policy.

Directive	Computers and Records	800-1	12 of 14
Effective Date	January 1, 2010		

I. Miscellaneous

1. The Records Management System contains files documenting arrests that occur within the Department's jurisdiction. The Department does not maintain separate hardcopy criminal history files on individuals arrested but in the Master Name Index in the RMS computer system is a link code that is assigned to that name. The results of a search on the Master Name index for a person will show all arrest and reports that are associated with that name.
2. Authorized personnel may access the arrest information in RMS however these files do not contain court dispositions and are not to be released to the public. Individuals inquiring about court dispositions should be referred to the Wilkes County Clerk of Court. The information contained within these files may be shared with other law enforcement personnel only.
3. Computerized Criminal History (CCH) transcripts may be obtained through the National Crime Information Center (NCIC) and the Division of Criminal Information (DCI). A criminal history may be requested for purposes of criminal investigations, criminal justice **employment** background checks. Wilkesboro Police Department is not authorized to run NCIC CCH for licensing purposes.
4. DCI certified operators may run criminal histories in accordance with this and DCI/NCIC regulations. Officers not certified shall request this information from the Administrative Assistant or another certified operator and personally receive any printed copies. Each request is automatically logged by DCI to provide accountability to the dissemination process, therefore each operator requesting a CCH shall include information in the request identifying dissemination to authorized persons or locations, such as the District Attorney's Office, outside the Wilkesboro Police Department.
5. Criminal history information from NCIC/DCI is not public information. Personnel receiving printed copies of this information will ensure that it is kept secure and not accessible to unauthorized persons. Unneeded printed copies will be shredded.
6. All information placed into any criminal process document shall be complete, accurate, and up to date. If errors are found the employee must notify his or her supervisor for the purpose of receiving authorization to lawfully correct the inaccurate data.

Directive	Computers and Records	800-1	13 of 14
Effective Date	January 1, 2010		

XII. TRAFFIC RECORDS

- A. Traffic accident data is recorded on state form DMV-349. This data is entered into the computer; the original hard copy is filed and maintained in Records. Copies of the accident forms are submitted to the North Carolina Department of Motor Vehicles on a monthly basis.
- B. Traffic enforcement data, citations, arrests, dispositions and locations are entered into the computer.
- C. Roadway hazard will be logged into the Activity Log section of RMS with a narrative stating the nature of the hazard and the action taken to correct and clear the hazard.
- D. Traffic accident and enforcement analysis reports are accessed through agency's computer system and North Carolina Division of Motor Vehicles.
- E. North Carolina Uniform Citation books are obtained from the Wilkes County Clerk of Court's Office.
- F. E-Citation will also be utilized by the Wilkesboro Police department.
- G. The Citation books shall be secured at all times while in the staff members possession. Each officer will be responsible for the citations they are issued and shall not leave them in unsecured areas.

XIII. OPERATIONAL FILES

- A. Case Files shall be maintained by Investigators until the case is disposed or inactivated then transferred to Records for consolidations with central records. (See Criminal Investigations - Purge Files)
- B. For additional security and control, case files of a sensitive nature such as Internal Affairs, Undercover Drug and Vice investigations, may remain in secured files separate from Central Records.

XIV. ARREST INFORMATION

When making an arrest, the arresting officer will complete the Arrest Report (DCI-608). Subjects arrested on felony charges shall be fingerprinted (one State Bureau of Investigation Card and 2 FBI cards,) and photographed. Subject fingerprinted at the Wilkes Intake Facility on the Live Scan system need submit only a copy of the fingerprints since the Live Scan automatically submits the

Directive	Computers and Records	800-1	14 of 14
Effective Date	January 1, 2010		

prints to the SBI. Subjects arrested for assault with a lethal weapon, all drug offenses, and any other violations the officer deems necessary may be fingerprinted and photographed with the exception of Chapter 20 violations. The information on the arrest report will be entered into the agency's computer system each time there is an arrest.

XV. WANTED PERSONS FILE

- A. Wanted persons are entered into NCIC whenever an officer deems it necessary to serve the warrant. The warrant must be physically checked at the agency to be entered into NCIC. Entries must contain appropriate suspect biographical/descriptive and other data as is required.
- B. When Wilkesboro Police Department receives a "Hit Confirmation Request" message from another law enforcement agency of a wanted person entered by this agency, a "Hit Confirmation" message will be returned via DCI (Division of Criminal Information) following the procedures mandated by DCI.
- C. Wanted Persons entered into NCIC are verified and validated monthly through the DCI validation process completed by the Administrative Assistant. Any NCIC entry that cannot be validated shall be cleared from NCIC. During the validation process the Administrative Assistant must verify that for each wanted person entry the warrant is still valid and in the possession of the department, or if returned, that the warrant is still valid, un-served, and obtainable.
- D. Warrants are entered into the agency's computer system upon receipt. Warrants can be cross-referenced in the master name index.
- E. Wanted persons are removed from NCIC when arrested or the warrant is physically removed from this agency, by returning un-served or transferring to another agency.
- F. Warrants are accessible to all agency law enforcement personnel 24 hours a day by computer generated search or by Document search. The original warrants are maintained in the records division for service. There is a printout of warrants currently on hand in the department, which is updated each time warrants are entered or removed from the RMS Warrant module.

XVI. REFERENCES

CALEA 1.2.5, 11.4.4, 82.1.1, 82.1.2, 82.1.3, 82.1.4, 82.1.5, 82.1.6, 82.1.7, 82.2.1, 82.2.2, 82.2.3, 82.2.4, 82.3.1, 82.3.2, 82.3.3, 82.3.4, 82.3.5 and 82.3.6