



# Town of Archer Lodge

## AGENDA

### Regular Council Meeting

Monday, December 2, 2024 @ 6:30 PM

Jeffrey D. Barnes Council Chambers

#### NCGS § 143-318.17. Disruptions of official meetings.

*A person who willfully interrupts, disturbs, or disrupts an official meeting and who, upon being directed to leave the meeting by the presiding officer, willfully refuses to leave the meeting is guilty of a Class 2 misdemeanor.*

Page

#### 1. WELCOME/CALL TO ORDER:

- 1.a. Invocation
- 1.b. Pledge of Allegiance

#### 2. APPROVAL OF AGENDA:

#### 3. OPEN FORUM/PUBLIC COMMENTS:

(Maximum of 30 minutes allowed; 3 minutes per person)

#### 4. ORGANIZATIONAL ITEMS:

- 4.a. Administration of Oath of Planning Board and Board of Adjustment Member(s) by Mayor Matthew B. Mulhollem
  - Christopher V. Cipriani
  - Francine Echols
  - John F. Oglesby

#### 5. DISCUSSION AND POSSIBLE ACTION ITEMS:

3 - 5

- 5.a. Discussion and Possible Action of Approving the Updated Electronic Communications and the Use of Town Property and Equipment Policy  
[Electronic Communications and the Use of Town Property and Equipment](#)

**6. TOWN ATTORNEY'S REPORT:**

**7. TOWN ADMINISTRATOR'S REPORT:**

**9. TOWN PLANNER'S REPORT:**

**8. HUMAN RESOURCES OFFICER/TOWN CLERK'S REPORT:**

**10. MAYOR'S REPORT:**

**11. COUNCIL MEMBERS' REMARKS:**

**12. ADJOURNMENT:**



## TOWN OF ARCHER LODGE

14094 Buffalo Road  
Archer Lodge, NC 27527  
Main: 919-359-9727  
Fax: 919-359-3333

**Mayor:**

Matthew B. Mulhollem

**Council Members:**

Clyde B. Castleberry

**Mayor Pro Tem**

Teresa M. Bruton

J. Mark Jackson

James L. (Jim) Purvis, III

Mark B. Wilson

# Electronic Communications and the Use of Town Property and Equipment Policy

This policy applies to all Town of Archer Lodge employees, elected officials, and appointees. The Town maintains electronic communication systems (e.g. voicemail, email, internet access) and provides access to telephones, computers, tablets, cell phones, or other electronic equipment to assist employees while conducting business for the Town. Access to the Town's electronic communication systems and devices requires certain responsibilities and obligations and is subject to relevant Town policies and local, State, and Federal laws.

These electronic communication systems and devices are for business use. Any personal use is limited to reasonable and appropriate use. Brief occasional personal use is permitted if it does not interfere with the user's work or anyone else's work at the Town, have a detrimental effect on the electronic communication systems' and devices' performance, incur any cost to the Town, result in loss of work time, violate or infringe on the right of any other person or entity, constitute a criminal offense or give rise to civil liability, and/or violate any Town policy or regulation. Personal use that is prohibited includes but is not limited to online auctions for personal purchases or sales, any use that would reflect negatively on the Town or its employees, playing games or engaging in on-line gambling, accessing, displaying, and/or transmitting sexually explicit material. Under no circumstances may employees use Town electronic resources and devices to access, receive, or send any material that might be considered offensive including but not limited to pornography, comments or images which could be considered offensive to someone based on their sex, race, religion, national origin, age, disability, or

genetics.

There will be no expectation of privacy for any information gathered, viewed, stored, or maintained on any electronic communication system or device.

The Town will not permit employees, elected officials, or appointees to view pornography on devices owned, leased, maintained, or otherwise controlled by the Town.

The Town will not permit employees to view pornography via the Town's electronic communication systems, including its internet network, regardless of what device is utilized, even if the Town does not own the device.

The Town shall report to the State Chief Information Officer, in the format required by the State Chief Information Officer, annually by August 1<sup>st</sup> of each year, all unauthorized viewing of pornography on the Town's network or devices.

Certain employees might need to view material that would be considered pornography in order to carry out their official job duties. The Town does not prohibit the viewing of pornography on a Town-issued device or network by any employee who is engaged in any of the following activities in the course of performing their official job duties:

- Investigating or prosecuting crimes, offering or participating in law enforcement training, or performing actions related to other law enforcement purposes;
- Identifying potential security or cybersecurity threats;
- Protecting human life;
- Establishing, testing, and maintaining firewalls, protocols, and otherwise implementing G.S. 143-805;
- Participating in judicial or quasi-judicial proceedings;
- Researching issues related to the drafting of analysis of state laws as necessary to fulfill the requirements of the employee's official duties.

Under North Carolina law, emails sent or received by the Town, except if considered confidential, is considered a public record and is subject to inspection on request by the public. All information created, stored, or transmitted on or with any Town resources is the property of the Town. The Town reserves the right to inspect or audit any documents, emails, or messages sent or received on the Town's equipment. Except as authorized by the Town, employees may not read or listen to any electronic communication intended for others.

Categories of information considered “Confidential” include, but are not limited to:

- Personnel records
- Criminal investigation records
- Legal matters
- Closed session minutes and general accounts
- Social Security numbers or personal financial information
- Contract bid documents until after the contract is awarded

Each employee is responsible for the security and integrity of Town information stored on the computer(s) assigned to the employee. The employee is responsible for controlling access to the electronic system, utilizing supplied virus protection software and ensuring the protection of personal passwords.