

Town of Apex

Policy Prohibiting Viewing of Pornography on Town Networks and Devices

December 10, 2024

BE IT RESOLVED by the Town Council of the Town of Apex that the following policies apply to the use of Town devices and Town networks.

I. PURPOSE

Session Law 2024-26, effective October 1, 2024, mandated that each public agency take affirmative action to adopt a policy prohibiting the viewing or accessing of pornography on Town networks and devices no later than January 1, 2025. This policy is adopted in satisfaction of this statutory requirement.

II. DEFINITIONS

- (1) Device – Any cellular phone, desktop or laptop computer, or other electronic equipment capable of connecting to a network.
- (2) Material – As defined in G.S. 14-190.13.
- (3) Network – Any of the following, whether through owning, leasing, maintaining, or otherwise controlling:
 - a. The interconnection of communication systems with a computer through remote or local terminals, or a complex consisting of two or more interconnected computers or telephone switching equipment.
 - b. Internet service.
 - c. Internet access.
- (4) Pornography – Any material depicting sexual activity.
- (5) Sexual activity – As defined in G.S. 14-190.13.

III. PROHIBITED USE OF TOWN NETWORK AND TOWN DEVICES

1. Notwithstanding N.C.G.S 14-456 and N.C.G.S. 14-456.1, no employee, elected official, or appointee of the Town of Apex shall view pornography on any device owned, leased, maintained, or otherwise controlled by the Town.

2. Notwithstanding N.C.G.S 14-456 and N.C.G.S. 14-456.1, no employee of the Town shall view pornography on any network owned, leased, maintained, or otherwise controlled by the Town, whether on a device controlled by the Town or on a privately owned, leased, maintained, or otherwise controlled device.

IV. EXCEPTION

Paragraphs 1 and 2 of Section III of this policy shall not apply to an employee or official that, in the course of that official's or employee's required job duties, is engaged in any of the following activities:

- (a) Investigating or prosecuting crimes, offering or participating in law enforcement training, or performing actions related to other law enforcement purposes.
- (b) Identifying potential security or cybersecurity threats.
- (c) Protecting human life.
- (d) Establishing, testing, and maintaining firewalls, protocols, and otherwise implementing this section.
- (e) Participating in judicial or quasi-judicial proceedings.
- (f) Conducting or participating in an externally funded research project at one of the constituent institutions of The University of North Carolina.
- (g) Researching issues related to the drafting or analysis of the laws of this State as necessary to fulfill the requirements of the employee's official duties.

This Policy shall not apply to the user of an authorized account paying for use of communications services under Article 16A of Chapter 160A of the N.C. General Statutes, including those communications services exempted under N.C.G.S. 160A-340.2(b) or (c).

V. REPORTING

1. Annually, no later than August 1 and in the format required by the State Chief Information Officer, the Information Technology Director or designee, shall report information to the State Chief Information Officer on the number of incidences of unauthorized viewing or attempted viewing of pornography on the Town's network; whether the unauthorized viewing was by an employee, elected official, or appointee; and whether or not any of the unauthorized viewing was on a device owned, leased, maintained or otherwise controlled by the Town.
2. Any employee of the Town who becomes aware of a violation of any provision of this policy shall report the violation to either the Human Resources Director or the Town Manager. If the violation was by an appointee of the Town Council, the Town Manager shall report the violation to the Town Council.

VI. VIOLATION OF POLICY

1. Any employee of the Town who violates any provision of this policy shall be subject to disciplinary action under Section 7 of Article IX of the Town's personnel policy.
2. Any appointee of the Town who violates any provision of this policy shall be subject to removal by the Town Council.

VII. IMPLEMENTATION OF POLICY

1. This Policy is in addition to and does not repeal, replace, or supersede IT Policy Procedure 300: "Policy on Information Technology" or Administrative Policy Number 103: "Cell Phone and Mobile Device Policy."
2. If any provision of this policy or any rule, regulation, or order thereunder of the application of such provision to any person or circumstances is held invalid, the remainder of the policy and the application of such remaining provisions of this policy of such rules, regulations, or orders to persons or circumstances other than those held invalid will not be affected thereby.
3. The Town Council has the authority to amend, revise, or repeal all or any portion of this policy as it sees fit.

VIII. EFFECTIVE DATE

This policy shall become effective on December 10, 2024.