

# SOUTH PORTLAND FIRE DEPARTMENT

## STANDARD OPERATING GUIDELINES

<b>Policy #:</b>	5.209	<b>Effective Date:</b>	3/6/2024
<b>Title:</b>	Computer & Internet Use	<b># of pages:</b>	3
<b>Category:</b>	Personnel	<b>Classification:</b>	Green

1. **PURPOSE:** To provide employees with general requirements for utilizing the City's computers, networks, and internet services.

These rules provide general guidelines and examples of prohibited uses for illustrative purposes but do not attempt to state all required or prohibited activities by users.

Failure to comply with this policy, these rules and/or other established procedures or rules governing computer use may result in disciplinary action, up to and including discharge. Illegal uses of the Department's computers will also result in referral to law enforcement authorities.

### 2. **POLICY:**

#### A. Access to City Computers, Networks and Internet Services

The level of access that employees have to the City's computers, networks and internet services is based upon specific employee job requirements and needs. The computer system is city property and intended for municipal business. All data and other electronic messages within municipal computers and servers are the property of the City of South Portland. E- mail messages and computer use records have been found to be public records and may be subject to the right-to-know laws, depending on their content.

In addition, the Department, through its Chief of Department and Chief Officers, reserves the right to review the contents of employees' e-mail communications and records of computer use when necessary for Department business purposes. Employees may not intentionally intercept, eavesdrop, record, read, alter, or receive other persons' e-mail messages without proper authorization.

#### B. Acceptable Use

Employee access to the City's computers, networks and Internet services are provided for administrative, educational, communication and research purposes.

General rules and expectations for professional behavior and communication apply to use of the City's computers, networks and Internet services.

Employees are to utilize the City's computers, networks and Internet services for Department related purposes and performance of job duties. Incidental personal use of City computers is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications.

Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules.

### C. Prohibited Use

The employee is responsible for his/her actions and activities involving City's computers, networks and internet services and for his/her computer files, passwords and accounts. General examples of unacceptable uses, which are expressly prohibited, include but are not limited to the following:

1. Any use that is illegal or in violation of other Department & City policies, including harassing, discriminatory or threatening communication and behavior, violations of copyright laws, etc.;
2. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive.
3. Any inappropriate communications with students or minors;
4. Any use for private financial gain, or commercial, advertising or solicitation purposes;
5. Any use as a forum for communicating by e-mail or any other medium with internal or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-department-sponsored organization; to solicit membership in or support of any non-department-sponsored organization, or to raise funds for any non-department-sponsored purpose, whether for-profit or not-for-profit. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the Chief of Department.
6. Opening or forwarding any e-mail attachments (executable files) from unknown sources and/or that may contain viruses;
7. Any malicious use or disruption of the City's computers, networks and Internet services or breach of security features;
8. Any misuse or damage to the City's computer equipment;
9. Misuse of the computer passwords or accounts (employee or other users);
10. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct;
11. Any attempt to access unauthorized sites;
12. Failure to report a known breach of computer security to the Chief of Department;
13. Using City computers, networks and internet services after such access has been denied or revoked;
14. Any attempt to delete, erase or otherwise conceal any information stored on a City computer that violates these rule

### 3. REFERENCES:

- CEFD SOG

- SPFD Bulletin 2012-01
- City of South Portland Computer Use Policy

By Order Of:

A handwritten signature in black ink, appearing to read 'Phil Selberg', with a stylized flourish at the end.

Phil Selberg  
Fire Chief