Seattle Police Department Manual

12.040 – Department-Owned Computers, Devices, & Software

Effective Date: 10/01/2021

12.040-POL-1 General Policy

The Department follows the City's Information Systems Security Policy.

Employees using Department-owned devices or software will follow the City's security policy:

- Protect and never share access accounts, privileges, and associated passwords

- Maintain the confidentiality of sensitive information to which they are given access privileges

- Accept accountability for all activities associated with the use of their network accounts and related access privileges

- Ensure that use of City computers, email, and other electronic communications (IM, etc.), Internet access, computer accounts, networks, and information stored, or used on any of these systems is restricted to authorized purposes and defined use limitations

- Maintain information security awareness

- Report all suspected security and/or policy violations to an appropriate authority (e.g., manager, supervisor, system administrator or the Office of Information Security)

For this policy, the term device means any electronic equipment that has the capability to:

- Connect to the internet or Department computer network and/or;

- Be used as a means of communication

For this policy, the term "non-standard technology" means all projects, contracts, surveys/forms, open datasets, and technology

acquisitions that are not formally identified City-wide standards, including, but not limited to:

- Free SaaS subscriptions,
- Contracts and professional services,
- IT projects,
- Open datasets, or
- Surveys

Exception: This policy does not apply to devices being used while conducting undercover operations. Employees will refer to their unit guidelines when using undercover devices.

12.040-POL-2 Protecting Department Hardware, Software and Computer Systems

The City's Information Technology Department (ITD) ensures the security of computer systems and software. ITD will audit and monitor the use of the equipment and access to information.

1. Only Authorized Users Operating Authorized Devices May Access the Seattle Police Department's Computer Network

Employees will access the SPD network only with devices authorized by ITD.

- This requirement includes devices used by other agencies assisting SPD or vendors working with ITD.

2. ITD Controls Department-Owned Software

ITD will review and evaluate purchases of computer and device software. ITD will approve or reject the purchase of software based on internal policies and the City's ITD guidelines.

ITD will maintain the software licenses for Department-owned software.

3. ITD Monitors Software Use on Department Devices

ITD will audit the software used on Department computers and will remove unauthorized software.

4. Employees Will Not Violate the License Agreement of Department Software

Employees will not copy Department-owned software or install the software on any other computer.

5. Employees Will Not Install or Download Non-Department-Owned Software, Applications or Programs on Department Devices

6. With Approval from their Lieutenant/Civilian Equivalent or Above, Employees May Request New Applications and Software (Including Free Technologies) by Completing a Request in the Seattle IT Service Hub

This is required for all requests to change any kind of IT system including, but not limited to, changes in hardware, network connections, addition or removal of applications, and additions or changes in application configurations, data elements, check lists, and drop-down lists.

Non-Department-owned software cannot interfere with the operation of any Department-owned software or hardware.

The unit assigned the software will maintain the license agreement. A copy of the license agreement is sent to ITD by the unit.

12.040-TSK-1 (below) contains the link to the service hub.

7. With Approval from their Lieutenant/Civilian Equivalent or Above, Employees May Request New Purchases of Non-Standard Technologies

This is required for all requests for any purchase of non-standard technologies.

(See 12.040-TSK-2 Requesting New Purchases of Non-Standard Technologies)

8. Employees Will Report Malfunctions of IT, Systems or Software by Calling the Seattle ITD Service Desk at 4-HELP to Complete a HEAT Ticket

Seattle ITD (previously known as DoIT help desk) is available M-F, 8-5 for routine desktop equipment or software related issues.

Seattle ITD can be reached via telephone at 4-HELP or 386-4011, or via e-mail at 4-Help@seattle.gov.

After hours assistance can also be requested via 4-HELP or 386-4011. After hours requests are handled by the on-duty Seattle ITD personnel.

Seattle ITD assistance via SPD Radio is also available 24/7 via Zone 2 / ITS. This resource is for in-car equipment issues related to the VMDT. Assistance is also provided to patrol officers that need a password reset to complete their patrol related tasks.

9. Employees Will Not Use Unauthorized Encryption Tools on a Department Computer or Device

10. Employees Will Not Password-Protect a Work File or Hard Drive

Exception: A lieutenant or above may authorize an employee to password-protect a file or drive based on an investigative or operational need.

Exception: This does not apply to Department-required passwords for Department computers, programs, or devices.

12.040-POL-3 Using Department Devices

1. Employees Have No Expectation of Privacy When Using a Department Device

The Department has the right to review all records related to Department devices including, but not limited to phone logs, text messages, photographs, email, and internet usage.

2. Employees Use Devices in a Professional Manner

Employees will use Department devices to communicate in a professional, appropriate, and lawful manner both on and off-duty.

Employees are accountable for all transmissions made on Department devices.

3. Personal Use of Department-Provided Devices Must Follow Department Guidelines

The Department allows limited, reasonable, personal use of Department devices with the knowledge that all use of Department devices may be monitored and subject to public disclosure.

Personal use of Department devices must not:

- Be illegal,
- Incur a cost to the City,
- Interfere with work responsibilities,
- Disrupt the workplace,
- Store unlicensed, copyrighted materials on any City-owned technology,
- Create a device-to-device connection between Non-City owned Technology and City-owned Technology,
- Comprise commercial or solicitation activities,

Or,

- Cause an embarrassment to the Department.

The Department may monitor and review all use of Department devices.

4. Department Devices Equipped with the VMobile Application Must Be Password Protected

Any use of the VMobile application must comply with manual section 12.050 - Criminal Justice Information Systems.

5. Employees Will Report Lost or Stolen Department Devices

In the event of a lost or stolen Department-issued device, the employee assigned the device must comply with 9.030-PRO-1 Reporting Destroyed, Lost, or Stolen Equipment.

6. Employees Will Not Access the VMobile Application in an Off-Duty, Unofficial Department Capacity

Off-duty use must comply with manual section 12.050 - Criminal Justice Information Systems.

7. The Act of Carrying a Department Device While Off-Duty Does Not, In Itself, Constitute Overtime

Overtime expectations vary by assignment. Supervisors will clarify their expectations for any off-duty use of Department devices. Unless an employee has been explicitly ordered by a supervisor to be available, check emails, or conduct other Department business outside of normal shift hours, they are not expected or encouraged to do so.

(See manual section 4.020-Reporting and Recording Overtime/Out-of-Classification Pay)

8. The Fiscal Unit Assists Employees with Cellular Phones

Employees making a request for a new or replacement cell phone will submit a 1.5 through their chain of command. Once approved, the Fiscal Unit will order the new phone and service.

9. The Department Telephone Coordinator Assists Employees with Desktop (Landline) Phones

Employees may contact the Telephone Coordinator at spd_telephone_coor@seattle.gov. The Telephone Coordinator can assist employees in the acquisition of phones and moving phone numbers to new locations.

Section Captain or civilian equivalent will approve the acquisition or moving of desk phones.

10. Employees Will Not Use Department Devices Internationally Without the Approval of a Captain/Civilian Equivalent or Above

After captain or civilian equivalent approval, employees will contact ITD to upgrade their device plan for international use.

International travel with a Department device may incur roaming charges to the Department.

11. Employees Will Comply with All Department Public Disclosure Requests

(See manual section 12.080 – Disclosure of Department Records)

12. When Receiving a Public Disclosure Request or Subpoena, Employees Must Retain All Requested Content

Employees will not delete requested items after receiving a public disclosure request or subpoena.

Department personnel may review content of any messages or photos contained on the device to make informed disclosure decisions.

13. Employees Will Retain Public Records According to the City Records Management Program

This includes, but is not limited to, text messages and photographs.

Employees seeking long-term retention may elect to transfer the content from the device to an appropriate Department network or system.

14. Employees Will Hold and Preserve All Public Records Relating to Litigation or Anticipated Litigation

Employees will hold and preserve all requested records until the City Attorney's Office releases the legal hold.

Employees will retain all records, including transitory records, responsive to a pending public records request until the Department's response to the request has been completed.

15. Employees Acknowledge that Public Disclosure Laws Apply to Personally Owned Devices Used for Department Business

Employees using their personally owned devices for official Department business and correspondence do so with the knowledge of this admonishment.

The Department prefers employees use Department-provided devices for Department-related matters.

Employees may request that their supervisor provide a Department-owned phone to make phone calls for official business.

16. The Department May Request Employees Review Their Own Personal Devices in Compliance with Public Disclosure Requests

The employee may be required to sign a declaration demonstrating the adequacy of the search of a personal cellphone or device regardless of whether the search resulted in responsive records.

Employees with questions regarding public disclosure may contact the Legal Unit.

17. Employees Will Not Charge Personally Owned Devices in Department USB Ports

Vehicle USB ports and USB ports that connect to a device may retain data from a personally owned device when plugged in.

Employees may use wall outlets or vehicle 12-volt DC sockets to charge personal devices.

12.040-TSK-1 Using the IT Service Hub to Submit a Request for Change or Enhancement Intake Request

To submit a change request approved by the chain of command, the **employee**:

1. **Navigates** to the Seattle IT Service Hub login page.
2. **Selects** the button next to "Sign in to one of the following sites:"
3. **Chooses** "Seattle IT Service Hub – PROD" from the dropdown list.
4. **Clicks** the Sign in button.
5. **Enters** his or her seattle.gov email address and network password to sign in.
6. **Clicks** "SERVICE REQUEST CATALOG" from the choices at the top of the page.
7. **Locate** the "Search for a Request Offering" field and **search** for SPD.
8. **Choose** "SPD Change or Enhancement Intake Request".
9. **Complete** the request and **submit** when finished.

12.040-TSK-2 Requesting New Purchases of Non-Standard Technologies

To request a new purchase of a non-standard technology, the **employee**:

1. **Obtains** approval from their lieutenant/civilian equivalent or above.

Once the request for purchase has been received from an employee, **lieutenant/civilian equivalent or above**:

2. **Contacts** the Technology Integrator to see if a privacy review is necessary

    - If a privacy review is necessary, the Technology Integrator and Performance, Analytics, and Research Section **completes** privacy paperwork and **submits** for review

3. **Completes** a 1.5 purchase order if a privacy review was not necessary