



DEPARTMENT OF PUBLIC SAFETY OPERATING PROCEDURES MANUAL		
CHAPTER 119	ELECTRONIC INFORMATION, COMPUTERS, AND COMMUNICATION	
	Effective: 8/15/2024	Commissioner Approval: 
	Authorities: AS 39.52 ; Administrative Order 81 ;	
	Applicability: ALL DEPARTMENTAL EMPLOYEES	
	Special Instructions: Click here to enter text.	

119.100 INTRODUCTION

The provisions of this Chapter apply to all information stored electronically on department or State equipment of networks, transmitted electronically (e.g. voice, data, facsimile, video or other forms) by employees while on-duty or using department or State equipment or infrastructure, and information accessed via department or State computers or networks.

All employees of the department, sponsored account holders, and any volunteers working for the department are bound by this policy. Violations of this chapter may lead to disciplinary action up to and including termination. Criminal sanctions may also apply to certain violations.

119.300 GENERAL RULES

A. ***Equipment, resources, and information to be used only for business purposes.***

Communications and computer equipment as well as network resources are to be used only for business purposes except where specific exceptions are provided. Employees and sponsored accounts shall be in compliance with [ISP 172](#). Information stored or transmitted electronically shall be viewed or used only for legitimate business purposes.

B. *No expectation of privacy.* Employees and sponsored account holders have no expectation of privacy for any electronic communications or computer files accessed using department equipment or resources. Supervisors or technical personnel may view, copy, monitor, record, archive, backup or otherwise manipulate computer files or electronic communications without notice.

C. *No use of department equipment or resources in support of political ventures or personal gain.* Employees are prohibited from utilizing department equipment or resources to support or oppose political candidates or parties, or in furtherance of any personal gain. This includes the use of email to lobby legislators or public officials on matters of personal political interest.

D. *Discriminatory, defamatory, harassing, or sexually explicit materials.* Except under the criminal investigation exception (See 119.330 C) the creation, editing, viewing accessing, or transmission of discriminatory, defamatory, harassing, or sexually explicit materials in any form is prohibited.

E. *Other Prohibited use of office technologies.*

1. Use for any purposes that violate a United States or State of Alaska law, including the Alaska Administrative Code.
2. Use for any commercial activities, including commercial advertising, unless specific to the charter, mission, or duties of the government agency.
3. Use for access to or distribution of indecent or obscene material or pornography.
4. Harassing other users, computer systems, and/or damaging or altering the software components of same.
5. Use for fundraising, political campaign activities, or public relations activities not specifically related to state government activities.
6. Any activity that adversely affects the availability, confidentiality, or integrity of any office technology.

F. *Rules applicable to all and at all times.* The rules in this chapter apply to any employee, sponsored account holder, or volunteer using state computer or network resources whether on or off duty, whether in a department facility or not.

G. *Identity not to be hidden.* Except as otherwise provided for in policy, employees may not intentionally hide their identity in email or Internet communications or access.

119.310 USE OF COMPUTERS AND COMPUTERIZED INFORMATION

A. *Personal computer software.* With few exceptions, software used on personal computers is not owned by the user, but the right to use a particular number of copies is licensed by the purchaser. Violators of software licenses can be subject to criminal penalties and can subject their employers to significant civil liability. It is the policy of the Department of Public Safety to respect all computer software copyrights and to adhere to the terms of all software licenses to which the department is a party.

1. Employees may not duplicate any licensed software or related documentation for business or personal use unless the department is expressly authorized to do so by agreement with the licensor.
2. Shareware software is copyrighted software that is distributed for a free trial period prior to payment of a licensing fee. It is the policy of the department to pay shareware authors the fee requested for any shareware products that are in use on department computers.
3. Any software for which proof of licensing (original disks, original manuals, or shareware receipts) cannot be demonstrated will be promptly removed from department computers. Supervisory or technical support personnel encountering unlicensed software during maintenance or other activities are authorized to immediately delete such software from department computers.
4. Personally owned software installed on department computers will be removed if it causes conflicts with department hardware or software, interferes with the ability of

any authorized user to access or utilize the computer, or occupies storage space needed by department owned software or data.

B. *Personal use of department computers.* Employees may not make personal use of department computers while on-duty. With prior supervisory approval, employees may make off-duty personal use of department computers for such purposes as the writing of academic papers or letters related to the professional development or advancement of the employee. Approved personal use of department computers must not be for financial or material gain.

C. *Improper use of computerized information.* Employees, sponsored account holders, or volunteers shall not make improper use of information contained in, or accessed through, department computers. Violators of this section may be subject to criminal prosecution, loss of computer access privileges, and/or discipline, up to and including dismissal. Improper use of computerized information includes:

1. Viewing computerized records without a legitimate business purpose for doing so (including for the purpose of satisfying curiosity).
2. Obtaining information in violation of law, regulation, policy, procedure, or other rule.
3. Release of records to any third party not legally entitled to the records.
4. Release of records to any third party not authorized by policy or procedure to receive the records.
5. Release or use of records for personal amusement or gain, or to benefit or cause injury to a third party or the department (including influencing political, electoral, or governmental decisions); and
6. Release or use of records for financial gain.

D. *No privacy expectation for DPS computer files.* Employees, sponsored account holders, or volunteers have no expectation of privacy for the files stored on DPS computers, networks, tapes, or removable storage media. DPS technical or supervisory personnel without notice beyond that provided by this policy may access these files. Upon request by a supervisor an employee shall provide keys or passwords to files that have been encrypted or password protected.

119.320 ELECTRONIC MAIL AND ELECTRONIC MESSAGING

When executive branch employees conduct state business through email they must, whenever feasible, use the state's electronic mail system. In some circumstances, employees may need to use, or inadvertently use, private email accounts to conduct state business. In those instances, employees must send copies of those messages to their state email accounts.

A. *Restrictions on the use of DPS E-Mail and TWIX communications.* DPS email and any other electronic messaging systems shall be used to conduct DPS business. The department may monitor electronic communications, and supervisors may, without notice beyond that provided by this policy, read messages.

- B. *There is no expectation of privacy for electronic messages sent or received on any state computer.*** Technical and/or supervisory personnel may view, print, copy, archive or otherwise access electronic messages at any time without notice to the employee.
- C. *Political activities.*** Email may never be used for political activities or in connection to profit making enterprises.
- D. *No discriminatory, defamatory, harassing or sexually explicit messages to be sent.*** Employees may not intentionally receive or transmit messages containing discriminatory, defamatory, harassing, or sexually explicit text, images, or multimedia.
- E. *Personal email messages limited.*** Employees may send or receive brief personal email messages so long as they do not disrupt the regular conduct of department business; they do not contain personal or intimate information that the employee would not freely share with supervisors and co-workers; and, they do not contain discriminatory, defamatory, harassing, or sexually explicit content.
- F. *Use of anonymous or false email addresses prohibited.*** Except with the permission of a supervisor during the course of an investigation, employees are prohibited from sending email from a DPS computer or terminal with a false address or using any service or technique intended to hide their true identity from the recipient of the message.
- G. *Record retention.*** Emails, including attachments, are subject to the same records retention requirements that apply to any other electronic or non-electronic records.

119.330 STATE SPONSORED EMAIL ACCOUNTS

In certain circumstances, non-department members may be provided a state sponsored email address to aid in conducting state related business effectively and securely. A state sponsored email should not be requested solely for convenience of the requestor or non-department member.

- A. *Warranted reasons for access or email requests.*** The purpose of granting non-department members access to a state sponsored email is to increase effective collaboration and exchange of secure information. Granting access should be limited and thoroughly considered.
- B. *Division Director Approval.*** All requests for granting a non-department member an email account must be approved by the unit/detachment supervisor and then the division director using the Department Sponsored Email Account User Agreement and Network Access Form. The approved form should then be attached to the technical support ticket requesting the account be created.
- C. *Use of Information.*** All information learned or obtained through a state sponsored email address is considered confidential and shall not be shared or otherwise disclosed without express permission from the sponsoring unit supervisor within DPS.

1. Sharing without permission from the department can result in account access of the sponsored account holder being revoked.
2. Revoking an account may preclude the sponsored account holder from fulfilling assignment duties. This may result in the sponsored account holder's agency evaluating whether the member can continue to perform in the current assignment (e.g. task force member). The sponsored account holder's agency will be responsible for identifying alternative means of secure information sharing if account access is revoked and for paying for the costs associated with those alternative means.

119.340 INTERNET ACCESS

- A. Access.** Internet access is provided so that employees may conduct the state's business. This includes access to Internet resources for the purposes of research, investigation, purchasing, or inter-governmental coordination.
- B. Privacy.** There is no expectation of privacy in any Internet access made using department computers or networks. The URL of each site visited is recorded and may be reviewed by technical or supervisory staff without notice to the employee.
- C. Access to certain Internet resources prohibited.** Other than for the purpose of investigating criminal or administrative violations, employees are prohibited from intentionally accessing any Internet resource containing discriminatory, defamatory, harassing, or sexually explicit content.
- D. Reported access.** Unintentional access to sites with prohibited content must be immediately reported to a supervisor. The site accessed, date and time, and circumstances should be part of the report to the supervisor.
- E. Procedures for intentional access to prohibited content.** Intentional access to sites with prohibited content for the purpose of criminal or administrative investigation shall be pre-approved by a supervisor and recorded in the appropriate report indicating the sites visited, date and time, and reason for access.

119.350 TELEPHONE PROCEDURES - GENERAL

- A. Answering phones.** Telephones shall be answered promptly and courteously. General access numbers shall be answered with the name of the division, department, or unit. Commissioned officers will identify themselves by rank and name when answering phones.
- B. Phone messages will be written.** All messages for employees not available to answer the phone shall be reduced to writing and routed according to local custom.
- C. Referral of callers to other numbers to be avoided.** All reasonable efforts will be made to assist the caller without requiring them to place another call. If the caller is reporting a crime, basic information and a call back number should be obtained, and the referral call placed

to the other agency by the member receiving the call. The caller should be advised of this procedure.

D. *Personal toll calls prohibited.* Personal toll calls will not be charged to department phones.

E. *Standards for use of voice mail.* Employees who have voice mail on their phones shall:

1. Record a message that includes the identity of the person or office reached, an invitation to leave a message, and instructions on reaching a human operator.
2. Check voice messages at least once each day the employee is at the workplace; and
3. Leave an explanatory message if the voice mail will not be checked for more than 3 days due to planned absence from the workplace.

Employees are encouraged, though not required, to update their messages daily (if appropriate) and to check their messages remotely if away from the office for a prolonged time while on-duty.

119.360 TELEPHONE PROCEDURES - DISPATCH

A. *Minimum information to be recorded for each service request.* Reports of crimes or requests for services received by dispatch will be documented by obtaining a case number for each occurrence. The following minimum information will be recorded for each service request:

1. Time received
2. Name, address, and home telephone number of the caller
3. Telephone number from where they are calling
4. Nature and details of service request
5. Exact location
6. Whether any special equipment is needed (e.g. ambulance, search and rescue, etc.), and
7. If available, the additional information needed to complete the dispatch card or service request form.

B. *Incident in progress calls.* If the caller is reporting an incident in progress, the caller should be kept on the line whenever possible. While the call is being dispatched to a unit on the road further information will be obtained, such as: what exactly is the caller seeing/hearing; suspect(s) name(s) and/or description; vehicle descriptions; suspect actions.

C. *Callout of standby Trooper in outlying areas.* Outpost telephones will be forwarded to the appropriate detachment dispatch center after hours. Each detachment is responsible for developing an S.O.P. to outline the types of calls for service requiring immediate callout of the standby Trooper.

D. *Screening of after-hours calls from outlying areas.* Dispatch centers will screen after hours calls forwarded from outlying areas to determine the need to recall the standby Trooper by applying the detachment callout policy established in paragraph C. Questionable calls or calls from citizens demanding to talk with a Trooper, will be directed to the on-duty Sergeant or OIC for the detachment area.

119.370 CELLULAR PHONE

A. *Acquisition of cellular phone services.* The acquisition of cellular phones and services are to be approved through the Division Directors who will assure that service is obtained at the lowest reasonable cost.

B. *Employees responsible for personal use.* Employees are required to reimburse the department for charges resulting from personal use on department cellular phones. Depending on the phone service contract this may require payment for all personal use including local calls, toll calls, and text messaging.

119.380 RADIO PROCEDURES

A. *During routine traffic only authorized 10-code to be used.* When using DPS radio channels during routine communications, all personnel will use the 10-code listed in section G. No other codes are to be used. Messages, which cannot be communicated clearly using the 10-code, should be conveyed in plain English.

B. *Emergency communications to be plain English.* During periods of declared emergency radio traffic, especially when multiple agencies may be involved, all transmissions on the emergency channel should be made in plain English. Dispatch should so instruct upon declaring an emergency channel.

C. *Transmissions to be brief.* All transmissions will be kept as brief as practical.

D. *Personnel to use assigned radio channels.* Personnel will utilize the specific channel assigned to them by Dispatch for the area or assignment, which they are working. When moving from one area to another, Dispatch will provide new channel assignments on request.

E. *Radio use to comply with FCC regulations.* All personnel will conform to the rules established by the FCC when using radio equipment.

F. *Radios to be repaired only by DPS APSCS.* Maintenance of department owned radio equipment is the responsibility of the Department of Public Safety, Statewide Services, Alaska Public Safety Communication Services (APSCS). Department personnel shall not repair, or attempt to repair, any State owned radio equipment without first coordinating with APSCS.

G. 10-code system to be used by DPS personnel.

10-1 Unable to copy	10-23 Arrived At Scene	10-79 Deceased
10-2 Signal is good	10-24 Assignment Completed	10-80 Prisoner In Custody
10-3 Change Frequency	10-27 Driver's License Check	10-81 Eating, Coffee
10-4 Acknowledge	10-28 Vehicle Registration Check	10-83 Unable to Locate/No Contact
10-5 Meet at/with (Location/Person)	10-29 Check Record for Wanted/Stolen Status	10-86 Providing Transport
10-6 Busy at (Location)	10-32 Firearm	10-87 Security/Bar Check
10-7 Out of Service	10-33 Emergency Radio Traffic Only	10-92 Clear for/Holding Confidential Information
10-8 In Service	10-36 Traffic Stop	10-93 Subject is Possible Health Hazard
10-9 Repeat	10-50 Motor Vehicle Collision D - D amage I - I njury F - F atality	10-96 Mental Subject
10-10 Fight in Progress	10-51 Wrecker	10-97 Negative Wants/Warrants
10-12 Stand By	10-55 DUI	10-98 Officer Safety Information
10-13 Weather	10-56 Intoxicated Person	10-99 Wanted/Stolen ADAM – A rmed/ D angerous F - F elony M - M isdemeanor L - L ocate
10-19 En Route to/Return to	10-60 Welfare Check	
10-20 Location	10-68 Officer Needs Routine Assistance	
10-21 Call _____	10-69 Officer Needs Emergency Assistance	
10-22 Disregard	10-77 ETA	

CHAPTER 119 ELECTRONIC INFORMATION, COMPUTERS, AND COMMUNICATION

H. *DPS radio designator prefixes.* Radio designators for individual officers using the DPS radio network are formed from three elements: a numeric code indicating the operational unit or agency (list follows); the alphabetic code of the Detachment/Bureau covering the officers assigned location; and a numeric identifier for the individual officer. For example: A Fire Marshal assigned to the B Detachment area might have a radio designator of 7-B-2.

1. AST	24. State Division of Parks
2. ABI/Narcotics	25. Kenai PD
3. Judicial Services	26. Wasilla Ambulance/Fire Departments
4. VPSO	27. Lakes Fire Department
5. AWT	28. Butte Fire Department
6. Probation/Pre-trial	29. Sutton Fire Department
7. FLS	30. USFWP Law Enforcement
8. Commercial Vehicle Enforcement	31. Alcoholic Beverage Control
9. Palmer PD	32. NTSB
10. Soldotna PD	33. Glennallen Fire/Medics
11. FBI/Secret Service/OSI/ATF/DEA	34. Bureau of Land Management
12. North Pole PD	35. US Immigration
13. Alaska Division of Emergency Services	36. US Customs
14. Public Safety Academy	37. Alaska Railroad
15. University of Alaska	38. Department of Treasury
16. Eielson AFB	39. Fort Yukon PD
17. Fairbanks PD	40. Alyeska Pipeline Security
18. Petersburg PD	41. Bethel PD
19. US Marshals Office	42. Homeland Security
20. Homer PD	43. US Coast Guard
21. Whittier PD	44. Department of Environmental Conservation
22. Seward PD	
23. Nenana PD	