



**Orientation Manual Page: 78**

We will not spend some times discussing policies and requirements related to technology. Not all employees within the department use technology at the same level. But there are some basic policies that apply to all employees.

**INTERNET ACCEPTABLE USE**

- ☐ Personal Use--use good judgment and in moderation
- ☐ Prohibited Activities
  - Pornography Sites – Adult Sites – Hate Sites
  - Violence Sites – Illegal Activity Sites
- ☐ Unauthorized Downloaded/Uploaded Software
- ☐ Blogging
  - Limited and occasional use is acceptable
  - Does not otherwise violate department policy
  - Is not detrimental to the department's best interests,
  - Does not interfere with an employee's regular work duties.
  - Employees may not attribute personal statements, opinions or beliefs to the department when engaged in blogging.
- ☐ External Access
- ☐ Reporting Problems

131

**Orientation Manual Page: 78**

Access to the Internet through the Department of Public Safety (DPS) network and computer systems opens a wide array of new resources and new services for its employees. However, these new opportunities also bring new risks. The Department controls Internet access to safeguard against a multitude of threats and grants access only to those employees who have a legitimate need for it. The ability to surf the web and engage in other Internet activities is not a fringe benefit to which all employees are entitled.

**Personal Use**

Employees are responsible for exercising good judgment regarding the reasonableness of personal use of the Internet. Moderate personal use of the Internet will be tolerated but excessive personal use is prohibited. Department of Public Safety policy does not allow for unrestricted personal use of the Internet. Users must adhere to other Department of Public Safety and State acceptable use policies which prohibits employees from visiting certain web sites at any time.

**Prohibited Activities**

With the exception of an authorized task or assignment, Department of Public Safety employees are strictly prohibited from visiting certain types of websites. The items listed below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use:

- Pornography Sites
- Adult Sites
- Violence Sites
- Hate Sites

- Illegal Activity Sites

### **Unauthorized Downloaded Software**

Bringing software from home or downloading unauthorized software and installing it on a DPS personal computer or network is strictly prohibited. However, if a legitimate business need exists for a particular file or piece of software, it must be approved and installed by appropriate IT personnel.

### **Unauthorized Uploaded Software**

No software shall be uploaded which has been licensed from a third party, or which has been developed by the Department to any other computer via the Internet. If a legitimate business need exists, it must be approved by the department.

### **Blogging**

Blogging by employees (e.g. Twitter) is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of department systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate department policy, is not detrimental to the department's best interests, and does not interfere with an employee's regular work duties. Employees may also not attribute personal statements, opinions or beliefs to the department when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the department. Employees assume any and all risk associated with blogging. Blogging from department systems is also subject to monitoring.

### **External Access**

With supervisory authorization and appropriate authentication, DPS employees wishing to establish a connection with the Department's network from an outside source such as an Internet Service Provider (ISP) via the Internet is acceptable.

### **Reporting Problems**

Immediate reporting of Internet security violations or problems to the Information Security Office is essential in order to affect prompt remedial action. Immediate reporting is necessary to limit losses from system penetrations and other potentially serious security problems. Delays in reporting can mean massive additional losses for the Department.

- Should sensitive material or data become lost, stolen, or disclosed to unauthorized parties, or is suspected of being lost, stolen, or disclosed to unauthorized parties, the user must contact the Information Security Office immediately. If passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen, or disclosed, the password must be immediately changed. The Information Security Office shall also be immediately contacted.
- Unusual system behavior, such as missing files, frequent system crashes, misrouted messages or other indications that the system has a computer virus infection shall be reported to the appropriate Helpdesk or the Information Security Office immediately.



**Orientation Manual Page: 79**

Email is a business communication tool, and users are obligated to use this tool in a responsible, efficient, and lawful manner. Although by nature Email appears to be a less formal means of communication, the same professional standards apply to Email as to other more formal written communication.

**Personal Use**

While minimal personal use of email will be tolerated, excessive personal use of email is prohibited.

**Privacy**

All messages distributed by any of the department’s email systems shall become the property of the Department of Public Safety. Users expressly waive any right to privacy in anything they create, store, send, or receive via Email.

**Violations**

Violations of this policy may result in revocation of privileges, restricted access to network systems, and/or other appropriate disciplinary action, up to and including dismissal. The Department of Public Safety reserves the right to monitor all network assets, including employee Internet usage.

## LAPTOP AND MOBILE DEVICE

- ▣ Data Encryption
- ▣ Attachments
- ▣ Links
- ▣ Bluetooth
- ▣ Disposal
- ▣ Thumb/Flash Drives

133

**Orientation Manual Page: 81**

Due to the greater likelihood for theft or loss, users should avoid storing confidential information on laptops or other portable media and devices whenever possible.

- Any mobile device (including a personally owned device such as a smartphone) that contains confidential information, DPS email, or other sensitive data, shall have the device and/or information encrypted using a department approved encryption method.
- Attachments should not be opened from untrusted sources.
- Links from untrusted sources should not be followed, especially from unsolicited email or text messages.
- Bluetooth functionality should be disabled if it is not in use.
- Data shall be removed before disposing of the device.
- The use of wireless devices to access the DPS network must be authorized by the DPS MIS division.
- In the event of theft or loss, DPS employees shall notify their management and the Information Security Office as soon as the theft is detected. Also, employees shall adhere to DPS policy for reporting misuse and/or theft of State property.
- Before a thumb/flash drive is connected to a DPS device, employees shall ensure that the appropriate security software (e.g. antivirus, antispyware, etc) is installed and current on the affected DPS device. Thumb/Flash drives with unauthorized/unapproved virtual operating systems are prohibited.

## COPYRIGHT INFRINGEMENT

- ▣ Employees shall obey licensing agreements and shall not install unauthorized copies of commercial software on agency technology devices.
- ▣ Copying software for any purpose other than making a back-up or archival copy is strictly prohibited unless prior written authorization has been obtained.
- ▣ Some license agreements restrict the use of software to certain equipment or devices. Unauthorized use of this software will be considered as unauthorized copying.
- ▣ The department does not require, request or condone unauthorized copying of computer software by its employees and violation of this policy may subject employees to disciplinary and/or legal action.

134

### Orientation Manual Page: 82

Unauthorized use of copyrighted computer software is a violation of federal copyright law, and a likely breach of this Department's license agreement with the software supplier. As a result, employees shall obey licensing agreements and shall not install unauthorized copies of commercial software on agency technology devices.

Copying software for any purpose other than making a back-up or archival copy is strictly prohibited unless prior written authorization has been obtained from the software manufacturer and appropriate Department of Public Safety officials.

Some license agreements restrict the use of software to certain equipment or devices. Unauthorized use of this software will be considered as unauthorized copying.

The department does not require, request or condone unauthorized copying of computer software by its employees and violation of this policy may subject employees to disciplinary and/or legal action.

## SOCIAL MEDIA POLICY

- ▣ NCDPS recognizes that its employees may use social media on a personal basis outside of their professional activities.
- ▣ A NCDPS employee who posts work related information on a social media site is still subject to the terms of this policy.
- ▣ Employees must clearly label and distinguish a personal opinion when it is publicly stated about NCDPS related matters.
- ▣ Personal social networking sites should remain personal.
- ▣ No use of state email account or password in conjunction with a personal social networking sites.

135

### **Orientation Manual Page: 82**

NCDPS recognizes that its employees may use social media on a personal basis outside of their professional activities and that such use may include the right to exercise freedom of speech. However, NCDPS encourages its employees to use good judgment when posting to a social media site as a private citizen, especially if the employee refers to anything related to NCDPS business. Employees must be mindful that they could blur their personal and professional lives when using social media. Even when acting away from the office in a private capacity, an employee must remember that he or she may be perceived by the public as representing the agency and state government as a whole when discussing NCDPS activities.

A NCDPS employee who posts work related information on a social media site is still subject to the terms of this policy. Employees must clearly label and distinguish a personal opinion when it is publicly stated about NCDPS related matters.

It is recognized that many NCDPS employees have personal social networking sites. These sites should remain personal. Employees should not conduct NCDPS business by way of any personal account. This helps to ensure a distinction between personal and agency views. Employees must not use their state e-mail account or password in conjunction with a personal social networking site. Employees may use personal social networking for limited family or personal communications while at work. Those communications should occur on break times and must not interfere with their work.



**Orientation Manual Page: 84**

This concludes your new hire orientation. We have covered a great deal of information related to departmental policies and procedures and your benefits.

Are there any questions regarding what we have covered?

You will need to complete the acknowledgement form and forward that to your supervisor to be placed in your personnel file at your work location. Your completion of this orientation program will then be entered in the Learning Management System (LMS). Once entered you will also have to complete an electronic acknowledgement in the Learning Management System. If you have questions about that process or have difficulty please talk with your HR Rep at your work location.

Thank you for your participation and your attention today and we wish you the best of luck with the Department.