

INFORMATION TECHNOLOGY/MIS

INFORMATION TECHNOLOGY POLICIES

INTERNET ACCEPTABLE USE

Location

<https://www.ncdps.gov/emp/Policies/ITPolicies/InternetAcceptableUse.pdf>

Policy

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.

Provisions

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 - Any site containing either graphic or text depicting, describing or otherwise endorsing explicit sexual acts, sex crimes, deviant sexual behavior, rape, sexual products or services, sexually provocative attire and gratuitous or full/partial nudity.
- Adult Sites - Any site containing profane and vulgar language, expletives, revealing attire, nudity, adult situations, or criminal activity.
- Violence Sites. Any site portraying or promoting injury, death or torture of human beings or animals, cult or ritual violence, suicide, malicious property destruction, and any site providing instructions on how to carry out these acts.
- Hate Sites - Any site that contains defamatory speech or activity directed towards a particular group based on race, ethnicity, religion, gender, or social status including sites operated by militant groups.
- Illegal Activity Sites- Under no circumstances is any employee, contractor or consultant authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Department of Public Safety owned resources

Unauthorized Downloaded Software

Bringing software from home or downloading unauthorized software and installing it on a Department of Public Safety 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, Department of Public Safety 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.

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.

EMAIL ACCEPTABLE USE

Location

<https://www.ncdps.gov/emp/Policies/ITPolicies/EmailAcceptableUse.pdf>

Policy

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.

Provisions

Email Usage

Any Department of Public Safety Email System should be used primarily for business purposes only. Employees and the department can be held liable for illegal or improper use.

- Users shall not send or forward Email containing libelous, defamatory, or obscene remarks.
- Users shall not use Department Email to vent negative emotions, or to send harassing, embarrassing, indecent, intimidating, or other unethical, immoral, or unlawful material.
- Users are prohibited from sending or forwarding messages that are likely to offend on the basis of race, gender, religion, national origin, age, or disability.
- Users may not send chain letters, junk mail, or personal files that utilize high bandwidth.
- Users are not allowed to use Email for private business activities.
- DPS managed email systems shall retain email records for a 10 year period.
- Unless authorized by DPS management, users shall not routinely use third party web mail accounts (e.g. Yahoo, Hotmail, Gmail, etc.) or other non-DPS email accounts to conduct DPS business. Users are responsible for retaining any email messages from web mail and/or personal email accounts that are used for state business. Users shall ensure that the aforementioned personal/web email messages are retained for a 10 year period.
- Users shall not attempt to forge or disguise their identity when sending Email.
- Users are prohibited from sending Email messages using another person's Email account unless they are a Proxy for a user that has granted them permission to send Email from their account.
- Users may not utilize an unauthorized method to encrypt an Email message without first obtaining written permission to do so from the IT/ MIS Section. Confidential or sensitive information shall not be transmitted via Email without the proper encryption enabled.
- Confidential or sensitive information shall not be put in the subject line of an Email (e.g. social security numbers). Email users should check with their supervisors if they are unsure about what to put in the subject line.
- Employees shall refrain from selecting unknown/untrusted Email links and /or opening untrusted/unexpected email attachments.
- Employees are reminded that the use of Department resources, including Email, should never create either the appearance or the reality of inappropriate use.

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 USE

Location

<https://www.ncdps.gov/emp/Policies/ITPolicies/LaptopMobileDevice.pdf>

Provisions

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. All Department of Public Safety (DPS) laptops shall have full disk encryption enabled and the encryption feature will be managed by the appropriate MIS personnel.

Backup media which is to be stored offsite shall be encrypted prior to delivery to the offsite storage facility and/or the offsite vendor.

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. If encryption is not feasible, other access controls (such as PINs, passwords, etc.) must be used. Additionally, mobile devices used to conduct DPS business must adhere to the following measures:

- When using password protection and if feasible, the password should contain a combination of letters, numbers, and special characters and have a minimum length of eight characters.
- 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 data removal method shall meet state standards when feasible.

Laptop and mobile device users will adhere to all relevant and applicable desktop security policies which include, but are not limited to, the following:

- Utilizing a timeout period for inactivity
- Logging off when systems are not in use
- Performing periodic backups of critical data
- Using only authorized software and programs (DPS owned devices)
- Complying with the DPS Remote Access policy
- Configuration and maintenance by authorized MIS staff (DPS owned devices)
- Vendor-supplied default and/or blank passwords shall be immediately identified and reset.

Mobile devices that have excessive storage capacity (e.g. external hard drives) shall adhere to the following guidelines:

- Network storage (e.g. SAN) shall be used in lieu of these devices when possible
- The DPS MIS personnel must review/approve the requisition for these devices
- Data encryption must be enabled – no exceptions

Laptop and mobile device users will take reasonable steps to physically secure unattended systems or media. Users will ensure that all laptop systems are updated and patched, at a minimum, on a monthly basis.

The use of wireless devices to access the DPS network must be authorized by the DPS MIS division. Wireless device access must adhere to any state and/or DPS wireless security requirements. Mobile devices such as Blackberries, smartphones, PDAs, etc. that are managed by the DPS MIS division or personal devices that store confidential DPS data will have the following controls enabled when possible:

- A maximum timeout interval of 10 minutes
- Password protection with the syntax rules requiring a combination of letters, numbers, and special characters
- Encryption of stored data
- Device location enabled
- Remote wiping enabled

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, antispysware, etc) is installed and current on the affected DPS device. Thumb/Flash drives with unauthorized/unapproved virtual operating systems are prohibited.

COPYRIGHT INFRINGEMENT

Location

<https://www.ncdps.gov/emp/Policies/ITPolicies/CopyrightInfringement.pdf>

Provisions

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

Location

https://www.ncdps.gov/emp/Policies/Communications/SocialMediaPolicy_08132013.pdf

Provisions

NCDPS recognizes the value of using social media, also known as new media or Web 2.0, as a way to communicate with stakeholders, media, its employees and the public at large. Tools such as Facebook, Twitter, YouTube and others are rapidly changing the way information is exchanged and governments are expected to engage the public using these Internet-based channels.

This policy will establish the following: 1) NCDPS position on the use of social media as part of its communication and customer service strategy; 2) guidelines and expectations for development and use of social media services in an official capacity; and 3) guidelines for employee's personal use of social media. These guidelines are applicable to NCDPS employees or contractors creating or contributing to blogs, microblogs, wikis, social networks, virtual worlds or any other kind of social media housed both on and off state-owned or operated servers. Any employee or contractor who participates in social media in an official capacity on behalf of NCDPS must follow these guidelines. These guidelines will likely evolve as new technologies and social networking tools emerge, so any employee or contractor who participates in social media in an official capacity on behalf of NCDPS must regularly check this policy to ensure compliance with it in its current form.

Use of Social Media to Represent Divisions/ Offices/Programs

NCDPS maintains official departmental social media sites and some of its subsidiary agencies also maintain their own separate social media sites. The Communications Office encourages subsidiary agencies to disseminate information by contributing to existing sites, as opposed to creating new social media sites. A few properly maintained sites that deliver consistently strong content are more effective than a diluted message delivered by a larger number of sites. Subsidiary agencies seeking to create new social media sites must have advance approval from the NCDPS Communications Office before launching a new site.

Creation and maintenance of all authorized social media sites will be conducted as part of a communications plan and strategy, as well as that of NCDPS. The NCDPS Communications Office will:

- I. Oversee decisions regarding social media sites including authorization of new sites;
- II. Verify staff being authorized to use social media tools;
- III. Maintain a list of social media domains, active account logins and passwords for every social media account authorized in NCDPS; and
- IV. Change passwords when an employee is removed as an administrator to maintain agency control.

Once a social media site has been authorized by the NCDPS Communications Office, agency communication officers or PIOs must monitor the site's establishment, content creation and maintenance to ensure that the mission and message are being appropriately articulated. At least two communications officers or PIOs from the communications office staff must have administrator rights on each NCDPS social media site. NCDPS social media sites must allow for public comment on the sites to promote open government, transparency, dialogue between constituents and to take full advantage of the benefits of social media.

Professional Use Guidelines

1. NCDPS related communication through social media outlets should remain professional in nature and should always be conducted in accordance with the agency's policies and expectations.
2. Creators, contributors and bloggers should stick to their area of expertise and provide unique, individual perspectives on what is going on at their divisions, and in other larger contexts.

3. Posts should be meaningful and comments should be respectful.
4. Spam or offensive remarks are not permitted. Communication should not include any forms of profanity, obscenity or copyright violations. Site administrators should remove comments that violate these rules as soon possible after they are noticed.
5. When a response is appropriate, comments will be responded to in a timely manner. A respondent should pause and think before posting a response. Generally, it is not appropriate to post personal opinions or discuss areas outside of one's expertise on a NCDPS social media site. An employee should always consider whether it is appropriate to commit oneself or one's agency to a course of action. If there is any question or hesitation regarding the content of a potential comment or post, it is better not to post.
6. Contact the Communications Office for guidance when responding to a sensitive or controversial post or when responding to comments that are critical of NCDPS.
7. Keep interactions appropriate and polite when it is necessary to disagree with others' opinions on NCDPS social media sites.
8. Proprietary information, content and confidentiality will be respected. Do not share confidential or non-public information.
9. Disclaimers addressing third-party ads and inappropriate content should be clearly visible on official sites where applicable.
10. Employees must not use agency social networking sites for political purposes, to conduct private commercial transactions or to engage in private business activities. Employees should be mindful that inappropriate use of social media can be grounds for disciplinary action. If an account is used for business, the entire account, regardless of any personal views, is subject to these best practices guidelines, including the collection and preservation provisions.

Employee Use of Social Media

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.

Personal Use Guidelines

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.