

Virginia Department of Social Services

Acceptable Use Policy

June 10, 2011

PURPOSE: To document the Virginia Department of Social Services' (VDSS) policy on the acceptable use of the Internet, e-mail, and other electronic communications.

SCOPE: All VDSS employees, employees of local departments of social services (LDSS), contractors, vendors, and volunteers and other persons and organizations that use VDSS sponsored Internet, e-mail and other electronic communications.

STATEMENTS OF POLICY:

General Statements:

1. Internet, e-mail, and other electronic communication users should have no expectation of privacy in regard to any message, file, e-mail, image or data created, sent, viewed, retrieved or received when using VDSS or Commonwealth of Virginia (COV) provided equipment or access. VDSS reserves the right to monitor computer networks, electronic communication systems, and the Internet at any time, without notice, and without the user's permission.
2. All electronic records may be subject to the Freedom of Information Act and available for public distribution.
3. All individuals and organizations that use VDSS-sponsored Internet, e-mail and other electronic communications will abide by the Department's policies and procedures.
4. Users of VDSS networks are prohibited from knowingly disclosing/sharing or modifying any assigned or entrusted access control mechanism (such as log-in identifiers, passwords, terminal identifiers, user identifiers, digital certificates, IP addresses, etc.) for any purpose other than those required to perform authorized employment functions.
5. Electronic communication systems provided by the COV to include computer systems, the Internet, e-mail, office phones, mobile cell phone devices, social media web sites and voice mail, are provided for official business and should not, as a matter of routine, be used for personal communications.
6. Users are expected to be responsible and professional when using COV-sponsored electronic communication services whether for personal or professional purposes.

7. If Directors wish to augment this policy with more restrictions they should first submit their planned restrictions to the VDSS Chief Information Security Officer (CISO) for review. This augmentation should clearly communicate to employees, in written form, their expectations on the allowable use of Internet, e-mail, and other electronic communication devices to ensure a clear understanding of unacceptable use if it is more restrictive than this policy.
8. Use of personally-owned equipment such as scanners, USB thumb drives, smart phones and computers to store and/ or process information that has been determined to be sensitive during a Risk Assessment or Business Impact Analysis is strictly prohibited and not allowed by COV Standards. If users are unsure of the sensitivity they should not process using personally owned devices. This requirement may be waived by VDSS during emergency situations.
9. Tools have been implemented by VDSS which:
 - Log Internet access.
 - Monitor Internet access and usage by individuals.

Internet Usage:

1. Acceptable use of the Internet consists of activities necessary to support the purpose, goals, and mission of VDSS and each user's authorized job functions as expressed in the Employee Work Profile (EWP).
 - Occasional and incidental personal use of the Internet services provided by VDSS is permitted during established lunch period (less than 15 minutes in any continuous hour), break periods (less than 5 minutes), before and after established work schedule (less than 15 minutes in any continuous hour), provided such use does not violate LDSS or COV policies, procedures or practices. This use can be further limited if it is determined to be detrimental to business use of the Internet.
 - Accessing personal e-mail through personal Internet Service Providers (e.g., AOL, Hotmail, Excitemail, Yahoo, etc.) at periods other than during established break/lunch time or before and after established work hours for periods of not more than a minute or two is also allowable (similar to personal calls on business phones). No attachments should be downloaded.
2. The following statements, although not inclusive, define specific unacceptable uses:
 - Accessing, downloading, printing, or storing sexually explicit material.

- Knowingly uploading or downloading commercial software in violation of its copyright and/or licensing agreement.
- Forwarding a Chain Mail.
- Gambling.
- Use for product or service advertisement.
- Unauthorized attempts to seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.
- Interfering with or disrupting network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, intentional propagation of computer viruses, and using the network to gain unauthorized entry to any other machine accessible through the network.
- Listening to radio, TV and other types of broadcasts (e.g., Webcasts, Streaming Video) that are not related to the employee's job duties and do not have prior supervisory approval. (Written approval required for Streaming Video)
- Downloading or /installing any of the following without written authorization from the (CISO):
 - Copyrighted materials (e.g., music and movie files)
 - Games to include playing games over the Internet
 - Screen Savers
 - Peer-to-Peer file-sharing programs
 - Non-VDSS supplied software
- If such use interferes with the conduct of VDSS and LDSS business or job performance (based on volume or frequency), involves solicitation or illegal activities, or adversely impacts the efficient operations of the agency's computer systems, the employee's access may be limited.
- At no time should personal use of the Commonwealth's provided Internet Services harm the agency or the Commonwealth, or involve for-profit personal business.
- The following are provided as examples of unacceptable use: routinely visiting Social Networking sites such as Face book, dating sites and Twitter accounts during established work periods for personal use.
- This policy does not attempt to define all unacceptable personal use. The above information is provided as a guideline. If the employee is unclear about acceptable personal use, they should seek the advice of their supervisor, Local Security Officer, or Director or contact the VDSS CISO for clarification.

E-mail Usage:

1. Any outbound e-mail sent using a VDSS or LDSS e-mail account is to be considered as equivalent to a message sent on agency letterhead. Therefore:
 - The content and tone of any such message must reflect the official responsibilities of the author; and
 - Any untrue, prejudicial, misleading, obscene, racist, sexist, or other unprofessional remarks that may make the organization liable for legal action or complaints of harassment or discrimination will be considered a breach of this policy.
3. It is prohibited to:
 - List a state e-mail address for personal endeavors or personal business use.
 - Send an e-mail using another's identity, an assumed name, or anonymously.
 - Use e-mail for the propagation of viruses, computer worms, Trojan Horses, and other malicious software.
3. If a suspicious e-mail is received, delete it without opening it and then empty the deleted mail folder.
4. Users may access their COV-provided e-mail from any personal computer, smart phone, I-Pad, or other devices, using the Internet. Users who remotely access any other agency resources will use only VDSS-provided equipment configured, set up and maintained by VITA or Northrop Grumman (NG) technicians without modification or similar equipment provided by a locality that is not supported by the Commonwealths' partnership with NG.
5. If an abusive, harassing or threatening e-mail is received, do not respond to it and report the incident to the Security Unit at security@dss.virginia.gov.

Acceptance and Violations of Policy

1. All users must acknowledge acceptance of, and continuing compliance with this policy, including the *Code of Virginia*, [§2.2-2827](#). Employees will further acknowledge that the VDSS Policy for Internet, e-mail, and other electronic communications may change from time to time and agree to abide by current and subsequent revisions of the policy. This acknowledgement will be made by all users by signing the Acknowledgement of Acceptable Internet, E-Mail and Other Electronic

Communications Use (see Attachment A) prior to being granted Internet, e-mail and other electronic communication access via VDSS facilities.

2. Known instances of non-compliance with this policy should be reported to the employee's supervisor/manager, HR and VDSS Information Security Office.
3. Violations of this Policy will be handled in accordance with established disciplinary procedures. Disciplinary action will be determined on a case-by-case basis by appropriate VDSS or LDSS management, with sanctions up to/or including termination depending on the severity of the violation.

AUTHORITY

REFERENCE: Code of Virginia, §2.2-2005, et seq.

(Powers and duties of the Chief Information Officer "CIO" Virginia Information Technologies Agency, "VITA")

Code of Virginia, §2.2-2009, et. seq.

(Additional duties of the CIO relating to security of government databases)

Code of Virginia, §2.2-2827

(Restrictions on state employee access to information infrastructure)

Code of Virginia, §2.2-1201.13

(Duties of the Department [Human Resource Management])

OTHER

REFERENCE: DHRM Policy No. 1.75, Use of Electronic Communications and Social Media.