

ELECTRONIC MEDIA USE

Effective Date: **October 1, 2017**

SCHRA requires all persons with access to Agency Internet, intranet, and e-mail systems are responsible for seeing that they are used properly and in accordance with the following policy. Questions concerning the policy should be directed to the SCHRA Network Administrator.

1. The Internet, intranet, and e-mail systems are for business purposes. Conducting personal business including accessing social media should be limited to non-working hours such as lunch breaks and before or after work.
2. Employees using the Agency's electronic media are expected to comply with all aspects of our Policy and Procedures. At no time should any subject matter of a sexual or violent nature be viewed, printed, or distributed.
3. The Agency may block Internet sites or protocols that the Agency deems to be inappropriate or may contain the risk of harmful or malicious programs. A site that is not blocked should not necessarily be considered acceptable. Employees must immediately leave inappropriate sites they encounter.
4. There is no personal privacy in any material created, received, or sent from the Internet or e-mail system. SCHRA, at its discretion, reserves the right to monitor and access any matter created in, received through, or sent from the Internet or e-mail system.
5. Messages sent during working hours should be sent only with good business reason for doing so. Copies should be forwarded only for good business reasons.
6. Each employee is responsible for the messages that are sent from his/her computer. Employees with e-mail passwords should not share their passwords with anyone. Passwords are to be kept strictly confidential.
7. Sending e-mail messages under an assumed name or obscuring the origin of an e-mail message sent or received is strictly prohibited.
8. All e-mails must follow Agency policy banning solicitation and distribution. Chain letters, pyramid schemes, promoting political or religious beliefs or tenets, and other solicitations are prohibited.
9. Employees are prohibited from engaging in any communication that is in violation of federal, state, or local laws.
10. No e-mail that constitutes intimidating, hostile, or offensive material on the basis of race, color, religion, sex, national origin, age, disability (physical or mental), veteran status, pregnancy, marital status, medical condition, sexual orientation, gender identity or any other status protected by federal, state, or local law or regulation may

be created, sent, or received at any time. SCHRA's policy against harassment applies fully to the Internet and e-mail system.

11. The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. Employees are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights.
12. To ensure a virus-free environment, no files may be downloaded from the Internet unless the origin of the message is known. E-mail messages and attachments should not be opened unless the sender is known to the receiver.
13. Employees should not access electronic data such as Agency maintained databases, e-mail, etc. with any other user's access codes than their own. User accounts and passwords should be confidential and staff should follow the Electronic Use Policy, maintained by the IT Department, when using electronic devices used to perform day-to-day operations requiring the use, access and maintenance of computer programs used by Agency.
14. All confidential information sent over external networks by any means must be encrypted with approved Agency technology. Certain types of transmissions may require additional controls. Please contact the Network Administrator for further guidance.
15. Employees must not disclose any Agency confidential or internal information on external bulletin boards, blogs, web pages, instant messages, etc., without an Agency's executive approval. This applies to all social media sites and other similar types of external locations.
16. Employees must not stream audio from the internet, use stock tickers, partake in internet gaming, or use systems in a manner that interferes with normal business functions in any way.
17. SCHRA purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, neither SCHRA nor any of its employees may reproduce such software for use on more than one computer.
18. Employees who become aware of misuse of the Internet, intranet, or e-mail system should promptly contact the Network Administrator and the Human Resources Director.
19. Any employees in violation of this policy are subject to disciplinary action, up to and including termination.

I hereby acknowledge review, receipt and understanding of the SCHRA Electronic Media Use Policy, above.

Employee Signature

Date