05. INFORMATION MANAGEMENT

5.1. Computers and Information Systems Acceptable Use

BOS Approved - Dec 20, 2017

(Employee retains this policy document)

5.1.1. Purpose. This policy exists to protect the County from inappropriate use of its computer and information systems, virus attacks, other compromises of security, and legal and related issues.

5.1.2. Definitions

A. The County's "computer and information systems" include, but are not limited to, all County-owned or leased: computer equipment, telephones, fax machines, printers, copiers, scanners, cell/mobile phones, iPads, laptops, pagers, personal digital assistants, network devices, software, hardware, storage media, data, peripherals and accessories, and any similar devices, as well as electronic media and services that the County provides such as e-mail, voice mail, the Internet and Intranet, electronic files, downloads, uploads, podcasts, and wireless access devices.

B. The term "User" includes all persons who use or have access to the County's computers information systems, including but not limited to all County officers, employees, and certain non-employees such as volunteers and interns who may have access to the County's computers and information systems.

5.1.3. Access and Authorized Use. Access to the County's computers and information systems is restricted to appropriate individuals as determined by the County. Every attempt should be made to protect vulnerable information at every level. Users must follow general password creation and maintenance protocol, keeping passwords private, protected, and maintained at all times. Electronic communications should be accomplished with the same level of care, professional judgment, and discretion as paper documents. Users should not assume electronic communications are private. Use of the County's information systems is a privilege made available to Users to assist in the performance of their County duties or County business only. Activities that conform to the purpose, goals, and mission of Fluvanna County and to each User's authorized job duties and responsibilities are generally acceptable uses of the County's computers and information systems.

5.1.4. Unauthorized Use. Activities that do not conform to the purpose, goals, and mission of Fluvanna County or to each user's authorized job duties and responsibilities are unauthorized uses of the County's computers and information systems and are strictly prohibited. The following list, although not all-inclusive, provides some examples of unacceptable prohibited computer and information system uses:

A. Use for any illegal purpose, including communications which violate any laws or regulations;

B. Use to access, create, transmit, print, download, or upload material (including images or text) that is considered abusive, fraudulent, defamatory, obscene, indecent, or sexually oriented, or which may be construed as harassing, threatening, or discriminatory based on race, color, religion, sex, national origin, age, or disability;

C. Use for private business or secondary employment, private or personal, for-profit activities or for private or personal business and/or gain;

D. Access of any private, non-County e-mail accounts, unless necessary for conducting County business;

E. Use of internet radio or streaming audio or video except for those Users needing streaming audio or video for the temporary purpose of taking a class, professional training, teleconferencing, or other temporary function directly associated with their job with the County may have such limited use;

F. The installation or use of non-County hardware, such as personal computers, personal laptops, flash drives, or wireless access points on the County network;

G. Use for "political activities" as described in Virginia Code Sections 15.2-1505.2 and 15.2- 1512.2;

H. Intentionally seeking information about, obtaining copies of, or modifying files, other data, or passwords belonging to other Users except as may be consistent with the User's duties as a County employee or officer;

I. Interfering with or disrupting network users, services, or equipment. Such disruptions could include, but are not limited to, (1) distribution of unsolicited advertising or messages, (2) intentional distribution of computer worms or viruses, (3) using the network to gain unauthorized entry to another machine on the network, and (4) attempting to diagnose and fix computer related problems beyond your level of expertise;

J. Installing any programs, files, screensavers, etc. which is not authorized by Fluvanna County;

K. Seeking/exchanging information, software, etc. which is not directly related to one's duties and responsibilities. This includes the non-business related exchange of files, including "jpeg", "gif" or other image type files and "mp3" or other audio type files; and

L. Any use of someone else's log-on ID or password.

5.1.5. <u>Monitoring</u>. The monitoring, auditing, and inspection by the County of any and all information systems may occur at any time, without notice, and without the User's permission in order to ensure compliance with this and other County policies and guidelines. Users shall have no expectation of privacy when using County computes and information systems. Electronic

records are considered public records and may be subject to disclosure under the Freedom of Information Act.

5.1.6. Violations. Violations of this policy or violations of related federal or Virginia law shall be reported immediately to the County Administrator. Any employee found to have violated this policy or related policies may be subject to disciplinary action up to and including termination of employment. Any violations by employees shall be handled according to the County's applicable personnel policies.

5.1.7. Use of Another Network or Service. Use of another network or service will subject the User to that network or service's acceptable use policy which shall apply in addition to the requirements of this policy.

5.1.8. Written Agreement Required. All Users of computer and information systems are required to acknowledge acceptance of and intention to comply with this policy, by signing the attached User Agreements. Signed agreements will be forwarded to the IT Department, and a copy will be placed in the employee's personnel file.

Attachments:

Form 5.1A User Agreement - Computers and Information Systems
Form 5.1B User Agreement - IT System Confidentiality and Security
Form 5.1C User Agreement - Computer Remote Network Access (if applicable)