130.1 Purpose

This policy establishes the minimum standards for all County employees and volunteers to ensure the appropriate, responsible, and safe use of electronic communications regardless of the system utilized.

130.2 Applicability

This procedure applies to all full-time, part-time regular and part-time County employees, contractors, interns, on-call workers, and volunteers connecting to the County resources.

130.3 Responsibilities and Requirements

All County employees and volunteers must comply with this policy regardless of the system utilized. Any work related posting to the internet or intranet or E-mail system is a professional communication in your capacity as a County employee or volunteer. The tone must be professional and the content must be accurate.

Inappropriate or unauthorized use, including using the network, internet, intranet, or e-mail system in any fraudulent manner will result in disciplinary action.

A. Retention of Electronic Communication

Electronic communications to include emails, text messages and voicemails, shall be archived and retained by employees as defined by the Virginia Public Records Act and in accordance with the Library of Virginia Records Retention Schedules.

B. Acceptable Use

County issued electronic communication tools are provided to facilitate effective and efficient County operations. Authorized purposes may include occasional personal communications from the employee's workplace, when such communications are of short duration, and whenever possible, made before/after work or during lunch or authorized breaks.

The Acceptable Use Policy also applies to the use of personally owned electronic devices while at the workplace. Personal devices are not authorized

to be connected to a County-business network and should only be connected to the County's publicly accessible guest Wi-Fi connection.

Use of personally-owned electronic devices in the employee's work area is left up to the discretion of department management. Personal devices are not authorized to stream (internet radio, television, movies) using County-business networks during normal business hours. Use of streaming media on County devices is is prohibited during normal work hours unless deemed necessary for work-related functions (Ex. Music for exercise classes, how-to videos or special events).

C. **Use Requirements**

When using electronic communications , users shall:

1. Follow all applicable County policies. Users may not violate any provision of this policy, or any other policy, regulation, law or guideline as set forth by local, State or Federal law. This may include but is not limited to copyright laws, trademark laws, and other requirements.

2. Be responsible and professional in their activities.

3. Exercise the appropriate care to protect the County's electronic communication tools against the introduction of viruses, spyware, malware, or other harmful attacks. Check with the appropriate IT Staff prior to downloading or accessing a file or document if the source of the file or other circumstances raises doubts about its safety.

4. Maintain the conditions of security (including safeguarding of passwords) under which they are granted access.

D. Prohibited Use

The following activities are prohibited on County electronic devices unless required for law enforcement activities:

1. Intentionally accessing, viewing, downloading, uploading, posting, or transmitting information that is abusive, offensive, harassing, threatens violence, or that discriminates on the basis of race, color, religion, gender, national origin, age, or disability.

2. Intentionally accessing, viewing, downloading, uploading, posting, or transmitting sexually explicit material. Sexually explicit material includes any description of or any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting nudity, sexual excitement, or sexual conduct of any kind.

3. Operating a business, product advertising, or conducting business for profit or personal gain.

4. Use of County email is intended primarily for official County business. Personal use, if necessary, should be limited to incidental use and is subject to review and enforcement for abuse and misuse. County-owned email addresses cannot be used for non-work-related alerts/notifications/newsletters (Ex. Shopping alerts, electronic coupons, or other personal subscriptions).

5. Gambling.

6. Arranging for the sale or purchase of illegal drugs or illicit activity.

7. Communication with elected representatives or public or political organizations via County e-mail to express opinions regarding political issues outside of work-related communications.

8. Sending of Countywide e-mail or e-mail broadcasts without first obtaining approval by the County Administrator or his/her designee.

9. Reproduction or transmission of any material in violation of any local, State, Federal or international law or requirement, including material that does not comply with federal copyright or trademark laws and copying or reproducing any licensed software, except as expressly permitted by the software license.

10. Electronically transmitting confidential information outside of the County network to external sources.

11. Intentionally creating a computer virus and/or placing a virus on the County's network or any other network. Intentionally drafting, forwarding, or transmitting chain letters. Intentionally accessing a computer without authorization or by a means exceeding authorized access using the County’s network or any other network (Hacking).

12. Any attempt to gain access to any other system or user's personal computer data without the consent of the other system or user.

13. Intentionally circumventing security and control features associated with County filtering policies or other Internet policies by using publicly accessible Internet wireless networks (such as Verizon air cards or public Wi-Fi) from County devices for purposes other than approved, official County government business.

14. Downloading or installing software without IT Department approval.

15. Forwarding of County email which constitutes official County government correspondence to a personal email account (such as Yahoo, GMAIL, or other Internet based email accounts), which reduces the ability to routinely manage the content.

16. Any other use of the network that violates Prince George County policies or Code of Ethics.

130.4 Posting or Transfer of Confidential or Inappropriate Information

Sensitive or confidential information that needs to be protected for governmental business, legal, or regulatory reasons must not be posted to the internet or transmitted insecurely. County Employees shall use secure file and large file transfer protocols developed by the IT Director.

County personnel and volunteers are prohibited from posting or transmitting the following:

(1) speech or images containing obscene, vulgar, or sexually explicit activity or language;
(2) speech or images that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals;
(3) speech or images that reflect behavior that would reasonably be considered reckless or irresponsible;
(4) speech or images that reflect negatively on the County; and
(5) the discussion of sensitive, confidential, proprietary, or classified information.

Examples of social media or online postings which are inappropriate and for which an employee or volunteer may be disciplined include, but are not limited to, posts or comments that:

(a) impair the performance of your duties;
(b) impair discipline and harmony among coworkers;
(c) impair working relationships of the County;
(d) interfere with County business or operations;
(e) disclose confidential or sensitive information; or
(f) negatively affect the public perception of the County.

The employee or volunteer should be aware of their association with the County in online social networks. The employee or volunteer should assume that his/her speech and related activities on social media sites will reflect upon the County. The employee or volunteer shall not post, transmit, or otherwise disseminate any information to which they have access as a result of their employment unless it is already public information. The employee or volunteer should ensure their profile and related content is consistent with how they want to present themselves as a County employee or volunteer, appropriate with the public trust associated with the position, and consistent with County and departmental personnel policies.

The employee or volunteer is prohibited from posting department logos, uniforms, or anything else identifying the department or County on a social media site or web page in a manner that reflects poor judgment or unprofessional actions.

130.5 Disciplinary Action for Violation of this Administrative Policy

Violation of this policy shall result in disciplinary action up to and including termination and restitution for all repairs.

130.6 Ownership & Management of County Information

All County owned computer systems, hardware, software, and any related systems and devices are the property of Prince George County. These include, but are not limited to, network equipment, e-mail, documents, spreadsheets, calendar entries, appointments, tasks and notes which reside in part or in whole on any County computer system or equipment. Accordingly, information stored on such systems or devices is also County property and subject to review at any time. Employees and volunteers have no expectation of privacy in the use of County resources. Electronic mail records are accessible by the IT Department staff as necessary.

Additionally, the County Attorney, County Administration, Human Resources and the Police Department may have reason to review the electronic files of employees and volunteers, which may be shared with others as necessary for legal and/or policy enforcement reasons. All County department directors shall work through the Police Department, County Attorney or Human Resources to evaluate the need to review electronic records of an employee pursuant to an investigation. The Police Department, County Attorney or Human Resources Department may then request permission from the County Administrator or designee for the retrieval of records, and forward that permission to the Director of Information Technology or designee for processing. In the event that an employee or volunteer is unexpectedly unavailable for other than disciplinary reasons and access to the employee's/volunteer's records is needed to support the ongoing operation of the business, the department director may request access to the electronic records from the Director of Information Technology or designee.

As with any other data (whether for citizens or employees), computerized information maintained by the County is subject to federal, state and local laws. Any County business e-mail or other communications, regardless of origin, may be subject to disclosure under the Virginia Freedom of Information Act ("VFOIA"), the Privacy Protection Act, and judicial subpoena. Since privacy cannot be assured within email systems, confidential information shall not be transmitted by non-secure email.

130.7 Security of Prince George County Technology Resources

Users are responsible for the use of their user account and should take all reasonable precautions to prevent unauthorized persons from being able to use their account. No

one shall share their passwords. For business continuity and emergencies, exceptions may be granted with Director of Information Technology (or County Administrator) and Department Head approval. All passwords shall follow applicable County password management standards. It is the responsibility of every employee/volunteer to report suspected security breaches immediately to the IT Department by contacting the main phone number to report a suspected breach.

130.8 Filtering

The IT Department will install and maintain filtering software for all County computers. Internet filtering of County computers is in accordance with the prohibitive uses described in Section 130.3(D). Exceptions to the filtering requirement may be made on an individual employee basis for appropriate governmental purposes. Department Heads should forward such request in writing to the Director of Information Technology for approval, identifying the individual employee and/or physical personal computer requesting the exception and the reason the exception is needed. The IT Department will maintain a list of unfiltered devices and users, which shall be periodically audited. The filtering of County computers does not relieve persons from the requirements specified in this policy, nor does it provide a defense to violations of this policy.

The IT Department also maintains SPAM filters which automatically filters for and removes suspect or dangerous email from delivery and places them into a SPAM folder. Incoming e-mail that could be interpreted as SPAM may include, but is not limited to, unacceptable file extensions (such as .exe files), excessively large size file attachments, objectionable content based upon subject title, and recognized malware or virus signatures. End users are provided the capability to manage their SPAM folders, but should exercise extreme caution in removing items designated by the system as SPAM.