Issue Analysis Form

Date: January 12, 2021

Item: Administrative Policy Revisions

Lead Department(s): Human Resources

Contact Person(s): Corrie Hurt

Description and Current Status

Staff has revised the administrative policies entitled "Electronic Information, Internet and Network Resources" and "Wireless Devices" for the Board's consideration at the January 12, 2021 meeting.

Electronic Information, Internet and Network Resources – Some of the main points revised here are communication retention, acceptable use, and use requirements.

Wireless Devices – Some of the main points revised are: removal of reimbursement for personal wireless devices, some changes to device usage in regards to guest vs. county WIFI connection, and the addition of mobile device procurement, setup and usage in section 120.5 and employee separation in 120.6

Government Path

Does this require IDA action?	☐ Yes	☒ No
Does this require BZA action?	☐ Yes	☒ No
Does This require Planning Commission Action?	☐ Yes	☒ No
Does this require Board of Supervisors action?	☒ Yes	☐ No
Does this require a public hearing?	☐ Yes	☒ No
If so, before what date?	☐ Yes	☒ No

Fiscal Impact Statement

None.

County Impact

To clarify electronic network resource and wireless device policies for all employees.

Notes

R-21-

Board of Supervisors
County of Prince George, Virginia

Resolution

At a regular meeting of the Board of Supervisors of the County of Prince George held in the Boardroom, Third Floor, County Administration Building, 6602 Courts Drive, Prince George, Virginia this 12th day of January, 2021:

Present:	Vote:
Floyd M. Brown, Jr., Chairman	
Marlene J. Waymack, Vice-Chair	
Alan R. Carmichael	
Donald R. Hunter	
T. J. Webb	

A-1

On motion of _____, seconded by _____, which carried unanimously, the following Resolution was adopted:

RESOLUTION; PROPOSED REVISIONS; PRINCE GEORGE COUNTY PERSONNEL POLICIES; SECTION 120.1 THROUGH 120.6 ENTITLED *WIRELESS DEVICES* AND SECTION 130.1 THROUGH 130.9 ENTITLED *ELECTRONIC INFORMATION, INTERNET AND NETWORK RESOURCES*

WHEREAS the Prince George County Personnel Policy Manual has been reviewed by staff and it has been recommended that the revised policies entitled ***Wireless Devices*** and ***Electronic Information, Internet and Network Resources*** be reviewed and considered for revision in the County's Administrative Policies;

NOW, THEREFORE, BE IT RESOLVED that the Board of Supervisors of the County of Prince George, this 12th day of January 2021 does hereby amend the Prince George County Administrative Policies by approving the revisions to the policies entitled *Wireless Devices and Electronic Information, Internet and Network Resources* as requested.

A Copy Teste:

_____
Percy C. Ashcraft
County Administrator

COUNTY OF PRINCE GEORGE ADMINISTRATIVE POLICIES Prince George, Virginia	POLICY NUMBER: 120.1 through 120.6	Page 1 of 4
SUBJECT: Wireless Devices	SUPERCEED ~~March 1, 2010~~ February 25, 2015	DATE ISSUED: ~~February 25, 2015~~
	AUTHORIZATION: ~~Percy C. Ashcraft, County Administrator~~Board of Supervisors	

120.1 Purpose

This policy establishes the responsibilities for all County employees or their designee for the acquisition and use of county-issued or personal wireless devices.

120.2 Acquisition of Wireless Devices

Purchases of all county-issued wireless devices shall be approved by the County Administrator or his/her designee. The IT Department shall set the device and technology standards for the use of cell phones, smartphones, tablets and other mobile data devices.

~~**120.3 Alternative to County-Issued Cellular Phones**~~

~~The County Administrator or his/her designee may approve reimbursement of business use of a personal wireless device based on the circumstances of County job requirements.~~

~~120.4~~120.3 **Personal Wireless Device Usage**

Use of personal wireless devices to access county systems and conduct county business is allowed, within the provisions set forth below.

1. Approval: Department Directors must approve in advance the connection of the employee personal device to county applications and services (email, phone app, alerting systems, etc.)~~systems and networks~~, other than publicly available access methods.

2. ~~Agreement: Execution of the Employee Acknowledgement Form for this policy by employee shall be required before the use of personal wireless devices will be allowed.~~

~~3~~2.~~.~~ Connection Methods: Only Department of Information Technology (IT Department) approved methods for connecting to county network and systems through wireless devices will be permitted. Only County-owned devices are authorized to connect to wired/wireless networks that have internal server/system access. Personal devices are limited to wireless guest networks.

Any attempt to circumvent these methods or introduce new methods will be treated as a disciplinary matter in accordance with §29.1 – 29.8 of the Prince George County Personnel Policy Manual.

1. ~~4~~3. Charges: There may be additional charges for software and services to allow personal wireless devices access to county systems. These expenses will be borne by the department. This includes, but is not limited to licensing fees, annual support and maintenance charges.

~~5~~4. Mobile Device: Loss, theft, ~~or~~ damage, defacement or compromise of ~~employee owned~~ personal device shall be reported to the IT Department immediately. Employees are responsible for obtaining replacement hardware and service without significant down-time in the event of loss, theft or damage. ~~The lost, stolen or damaged device shall be subject to a remote wipe of county data from the device.~~

Commented [CH1]: IT doesn't have the ability to remotely wipe a personal device.

~~6~~5. Expense Responsibility: All charges incurred on personal wireless devices are the responsibility of the employee. ~~unless the device is covered by Section 120.3.~~ The Employee will bear the expense of the insurance and replacement cost of the device.

~~7~~6. Records Retention: It is the responsibility of the employee to ensure records retention guidelines are adhered to and that public records are protected. Employees should reference Administrative Policy entitled, "Records Retention," §210.1 – 210.4.

~~8~~7. FOIA: Communications, records and data stored, sent or received for the purpose of conducting county business is subject to the Freedom of Information Act (FOIA) and apply to both county-issued and personal wireless devices.

~~9~~8. Agreements: It is the responsibility of the employee to execute all agreements and commitments. Neither the county, IT Department nor any department shall be liable for any agreements or commitments the employee makes with wireless service providers.

~~120.5~~120.4 Miscellaneous Provisions for Use of County-Issued Wireless Devices

1. Hardware Issues: Loss, theft or damage, defacement or compromise of county-issued device shall be reported to the IT Department immediately. The lost, stolen or damaged device shall be subject to a remote wipe of county data from the device.

2. Suspension of Service: If a service is not needed temporarily, Department Directors can request by email with the ~~Finance~~ IT Department that wireless service be suspended for a period of time. Department Directors can request

by email with the ~~Finance~~ IT Department the reinstatement of wireless service at any time.

3. Disconnection of Service: If a service is no longer needed Department Directors shall email the ~~Finance~~ IT Department requesting service disconnection. Any fees associated with early disconnection of service are the responsibility of the department.

4. Returned Equipment: Equipment that is replaced or no longer needed must be returned to the IT Department, including all accessories (charging cables, case, etc.). Replacement of unreturned accessories will be the responsibility of the employee. The IT Department will review and erase data, if possible, or destroy the equipment and forward notice of such actions to the Finance Department.

5. Maintenance: In the event that maintenance is required, the employee will contact the IT Department for coordination with the contracted vendor.

6. Personal Use of County Devices: Personal use of County-owned devices ~~printer/copier equipment~~ is normally prohibited. However, Departments may permit occasional use of ~~printer/copier equipment~~County-owned devices by employees ~~for community or volunteer purposes~~ so long as such use furthers County policies supporting employee or volunteer activity and is limited to an insignificant volume, and does not result in additional costs/charges to the County.

~~120.6~~120.5 ~~Distribution of Wireless Devices Policy to County Employees; Employee Acknowledgement~~Mobile Device Procurement, Setup and Usage

~~A copy of the Wireless Devices Policy shall be distributed to each County employee with an Employee Acknowledgement Form. Each County employee shall acknowledge receipt of the Policy by signing and dating the Employee Acknowledgement Form in the presence of a witness who shall also sign and date the Acknowledgement. The executed Employee Acknowledgement shall be returned to the Department of Human Resources for filing in the respective employee's personnel file.~~

1. Mobile device purchases will be limited to low cost, technologically sufficient devices available through approved vendors.
2. Device upgrades will only be authorized when the current device is no longer able to meet technological requirements, or malfunctioning and unrepairable.
3. Mobile devices (phones, tablets, etc.) will be configured using an email address that is owned/managed by the County, and setup by the IT department.
4. Data plans should be limited to one data plan per authorized person, unless additional data plans would provide a significant benefit, or cost savings to the County.

120.6 Employee Separation

1. Upon separation, employee must provide their supervisor or the IT department with all pins/passwords required to unlock or reset their assigned County-owned devices.
2. County-issued phone numbers will not be transferred to employees for personal use under any circumstances.
3. County-owned devices will not be available for resale under any circumstances.

COUNTY OF PRINCE GEORGE ADMINISTRATIVE POLICIES Prince George, Virginia	POLICY NUMBER: 130.1 through 130.9	Page 1 of 7
SUBJECT: Electronic Information, Internet and Network Resources	SUPERSEDES: ~~March 12, 2007~~ June 10, 2015	DATE ISSUED: ~~June 10, 2015~~
	AUTHORIZATION: ~~County Administrator~~Board of Supervisors	

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 ~~managed by~~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~~whether connected~~ to a County-business network and should only be connected to ~~or using a~~ the County's publicly accessible guest Wi-Fi connection. ~~In areas where employees must share equipment or resources for network access, employees using the resources to fulfill job responsibilities always have priority over those desiring access for personal use.~~

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 ~~(such as Internet Radio)~~ on County devices is ~~also left up to the discretion of the department management~~is prohibited during normal work hours unless deemed necessary for work-related functions (Ex. Music for exercise classes, how-to videos or special events). ~~, unless it is determined by the IT Department that it creates a disruption or problem within the County network or on an individual workstation, in which case such use is prohibited.~~

C. **Use Requirements**

When using electronic communications ~~tools and social media~~, 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. When communicating or posting to social media, be clear that the communication or posting is personal and is not a communication of the County.~~

Commented [CH1]: This will be incorporated in the next social media policy changes.

~~4.~~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.

~~5.~~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. ~~Using County e-mail systems excessively for personal use.~~ 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.

~~**130.9 Distribution of Electronic Information, Internet and Network Resource Policy to County Employees; Employee Acknowledgment**~~

~~A copy of the Electronic Information, Internet, and Network Resource Policy shall be distributed to each County employee with an Employee Acknowledgement. Each~~

~~County employee shall acknowledge receipt of the Policy by signing and dating the Employee Acknowledgement form in the presence of a witness who shall also sign and date the Acknowledgement. The executed Employee Acknowledgement shall be returned to the Human Resources Department for filing in the respective employee's personnel file.~~