1. Overview

The County's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Campbell County's established culture of openness, trust and integrity. We are committed to protecting Campbell County's employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and File Transfer Protocols (FTP), are the property of Campbell County. These systems are to be used for business purposes in serving the interests of Campbell County, and of our clients and customers in the course of normal operations. Please review Public and Employee Relations policies for further details.

Effective security is a team effort involving the participation and support of every Campbell County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Campbell County. These rules are in place to protect the employee and Campbell County. Inappropriate use exposes Campbell County to risks including cyber attacks, ransomware, compromise of network systems and services, data breach, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Campbell County business or interact with internal networks and business systems, whether owned or leased by Campbell County, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Campbell County and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Campbell County policies and standards, and local laws and regulations.

Campbell County's network resources, as with any other public resource, demands that those entrusted with its use are accountable for that privilege. Therefore, it follows that use of the County's network resources must be in direct support of the assigned duties and responsibilities of the user in carrying out the business of the County. The right to have access is a management decision and access is subject to restriction for any employee misuse. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Campbell County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Campbell County.

4. Policy

4.1 General Use and Ownership

4.1.1 Campbell County private information stored on electronic and computing devices whether owned or leased by Campbell County, the employee or a third party, remains the sole property of Campbell County. You must ensure through legal or technical means that private information is protected.

1.1 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Campbell County private information.

1.2 You may access, use or share Campbell County private information only to the extent it is authorized and necessary to fulfill your assigned job duties.

1.3 To protect our organization's data and ensure the integrity of our network, the use of personal mobile devices to connect to corporate wireless networks is strictly prohibited. This includes smartphones, tablets, and any other personal devices that are not issued or authorized by the County.

1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for establishing guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

1.5 For security and network maintenance purposes, authorized individuals within Campbell County may monitor equipment, systems and network traffic at any time, per Campbell County's associated job requirements and position.

4.1.2 Campbell County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Private Information

4.2.1 Use of network resources must be supportive of organizational objectives and be consistent with the mission of Campbell County.

4.2.2 Sensitive or confidential information must not be input into Artificial Intelligence (AI) systems without prior authorization. Employees must ensure compliance with data privacy regulations.

4.2.3 Users must abide by copyrights, contractual arrangements, local, state, and federal laws and regulations, as well as the policies of Campbell County and any individual department's operating guidelines.

4.2.4 System level and user level passwords must comply with the *Password Construction Guidelines*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.5 To enhance the security of email accounts and protect sensitive information, Campbell County has implemented Multi-Factor Authentication (MFA) for all email accounts. This measure adds an additional layer of security by requiring users to provide two or more verification factors to access email accounts.

4.2.6 All computing devices must be secured with a password-protected lock screen mechanism with the automatic activation feature set to 15 minutes. You must lock the screen or log off when the device is unattended.

4.2.7 Postings by employees from a Campbell County email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Campbell County, unless posting is in the course of business duties.

4.2.8 To ensure the safety and security of our organization's data and systems, all employees are required to complete mandatory cybersecurity training. This training is designed to enhance awareness of potential threats, promote best practices for data protection, and equip staff with the necessary skills to recognize and respond to cybersecurity incidents.

4.2.9 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee, contractor, consultant, temporary, and other workers of Campbell County authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Campbell County-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Campbell County.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Campbell County or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server, or an account for any purpose other than performing instructed Campbell County duties, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, ransomware, etc.).

6. Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a Campbell County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any Campbell County account.

9. Making statements about offering or extending any warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this

section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to the Information Technology Department is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the Campbell County network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, Campbell County employees to parties outside Campbell County without proper consent.

18. Using Campbell County computing assets to view, procure, store, or transmit pornographic materials is strictly prohibited. Such activity violates workplace standards, undermines a professional environment, and may breach local, state, or federal laws.

4.3.2 Email and Communication Activities

When using County resources to access and use the Internet, users must realize they represent the County. Whenever employees state an affiliation to the County, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the County". Questions may be addressed to the IT or Public and Employee Relations Departments.

1. Freedom of Information – Information contained in an e-mail should be retained and disposed of the same as a paper record in accordance with the Virginia Public Records Act. For these records the user may wish to make a hard copy of the e-mail to be filed. Other e-mail, not considered a public record, may be deleted. (refer to Chapter 8 of the County Handbook, section 6&7 – Records Management Policy) Unless the e-mail is specifically exempted, it must be produced if requested under the Virginia Freedom of Information Act. Departments/Staff are responsible for familiarizing themselves with the Virginia Freedom of Information Act and the record keeping requirements related to their job function. If subpoenaed, e-mail records must be produced.

2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

4. Unauthorized use, or forging, of email header information.

5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

7. Use of unsolicited email originating from within Campbell County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Campbell County or connected via Campbell County's network.

8. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

1. Blogging as an employee or blogging on work related matters, whether using Campbell County's property and systems or on personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Campbell County's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Campbell County's policy, is not detrimental to Campbell County's best interests, and does not interfere with an employee's regular work duties. Blogging from Campbell County's systems is also subject to monitoring.

2. Campbell County's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any County related confidential or private information, trade secrets or any other material intended to not be public knowledge.

3. Employees shall not engage in any online activities, including but not limited to blogging, social media posting, or other forms of digital content creation, that may harm or tarnish the image, reputation, and/or goodwill of Campbell County and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments or engaging in conduct prohibited by *Campbell County's Employee Handbook and Code of Conduct*, whether online or offline.

4. Employees may also not attribute personal statements, opinions or beliefs to Campbell County when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Campbell County. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Campbell County's trademarks, logos and any other Campbell County intellectual property may also not be used in connection with any blogging activity

5. Policy Compliance

5.1 Compliance Measurement

The Information Technology and Public and Employee Relations departments will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the IT and PER departments in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- *Remote Access Policy*
- *Password Construction Guidelines*

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Private Information
- Spam
- Ransomware

8. Revision History

Date of Change	Responsible	Summary of Change
August 2018	Jonathan Pingilley	Adopted from SANs Security Policy Project
January 2025	Jonathan Pingilley Jodi Crews	Updated areas to reflect new technologies and policies