Acceptable Use

Contents

1. **Purpose** 1
2. **Applicability** 1
3. **Policy** 1
4. **Policy Non-Compliance** 4
5. **Audit** 4
6. **Definitions** 4
7. **Approval and Revision History** 6

1. Purpose

The purpose of this policy is to outline the acceptable use of the Buncombe County Information Technology (BCIT) Systems. These rules are in place to protect Buncombe County information system users as well as the County. Inappropriate use exposes Buncombe County to risks including virus attacks, ransomware attacks, theft, legal issues, and compromises network systems, services and data.

2. Applicability

This policy applies to all Buncombe County departments and employees. This includes all Buncombe County employees, volunteers, contractors, vendors, or third party's using a Buncombe County information system, device, or resource. Where there is conflict with any department-specific policy, this document will supersede.

This policy must be reviewed and signed annually by all employees.

3. Policy

3.1. Access to County IT Systems

3.1.1. Users must not purposely engage in activity that is illegal according to local, County or federal law, or activity that may harass, threaten or abuse others, or intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene such as sexually explicit materials. Access, storage, and transmittal of such content is permissible only insomuch as it is commensurate with the scope of a user's employment, such as conducting a legal investigation.

3.1.2. Actions and statements by users that are in violation of the Unacceptable Personnel Conduct Standards found in the Buncombe County Personnel Ordinance are still subject to disciplinary action even if they are not made with County equipment, IT Systems and accounts. This is inclusive of statements made on social media platforms.

3.1.3. The County recognizes that there are times when employees may use County devices for personal use. Personal use is permitted if: (a) the use is not against the law; (b) the use does not interfere with the performance of public duties including duties of both the employee and other county staff; (c) the cost or value related to

the use is nominal; (d) the use does not create the appearance of impropriety; and (e) the use is not in pursuit of the employee's private financial gain or advantage.

3.1.4. Users accessing the County network must only access streaming content as consistent with the mission of the agency for the minimum amount of time necessary.

3.1.5. Information technology (IT) resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, personal business ventures, solicitation or performance of any activity that is prohibited by any local, County or federal law or other conflicts of interest.

3.1.6. Users must not allow non-County employees to have access to non-publicly accessible information systems.

3.1.7. Each user should identify themselves honestly, accurately, and completely when using any technology medium. This includes telephone, email, social media, on-line user groups, or when setting up user accounts. Only those employees who are authorized to speak or write to the media on behalf of Buncombe County may do so in accordance with Buncombe County's Media Relations policy.

3.2. **Hardware**

3.2.1. Users are prohibited from connecting non-county issued devices to the county network. Users may connect non-county issued devices to the county guest wi-fi network and assume all risks in doing so.

3.2.2. All equipment should be maintained in an appropriate manner and always safeguarded from environmental damage such as immersion in water, exposure to direct flame or forceful impacts. Equipment should not be exposed to extreme hot or cold temperatures and should not be defaced in any way.

3.2.3. Users must always exercise care to preclude hardware theft. Mobile devices must never be left unattended.

3.2.4. Users must lock or power down computer equipment and devices when away from their workstation/desk or otherwise not in use to prevent unauthorized access.

3.2.5. If an employee ends their employment with Buncombe County, they are required to return all County-owned technology, equipment, and supplies within 3 business days of their last working day. Failure to return equipment will result in action including deducting the cost of the equipment from the employee's last paycheck in accordance with N.C. Gen. Stat. 95-25.8, and the County reserves the right to take action through any legal means for recovery of or compensation for such items.

3.3. **Software**

3.3.1. All new software applications, including Software as a Service (SaaS) applications, must comply with the Buncombe County Procurement Manual and be approved by the IT Director prior to acquisition. Applications that have been pre-approved for use can be accessed via the Buncombe County Software Center on a County device. Software listed under the "Applications" section may be installed by the end-user without IT intervention.

3.3.2. Software not accessible through the County Software Center must be requested through the Buncombe County's Service Desk System after supervisor or

Department head approval. This includes open-source and software advertised as free for use. If software is approved by the IT Director, BCIT will review software requests and make every effort to utilize existing software titles for consistency and support. BCIT will consult with applicable support departments as-needed for viable software options.

3.3.3. Users must not make unauthorized copies of copyrighted or County-owned software. Employees should use computer software only in accordance with applicable licensing agreements.

3.4. **Security & Reporting**

3.4.1. Buncombe County specifically prohibits security breaches or disruptions of network communication. Security breaches include but are not limited to accessing data without express authorization, accessing data that was received in error or accessing an Information Technology System without express authorization. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, packet spoofing and any form of denial of service (DoS) attack.

3.4.2. Sharing or lending any account password/pin/badge or other security or systems access is strictly prohibited.

3.4.3. Information stored on County computers or in County supported cloud applications is essential for county business operations and in some instances confidential. Use or distribution of such information, other than in the course of regular job duties, is prohibited by the County and may also be prohibited by state and federal laws.

3.4.4. Transmitting sensitive information should never be sent through unencrypted channels. The County provides email encryption and secure file exchange to securely transmit confidential information. More information on how to encrypt emails can be found here:
https://servicedesk.buncombecounty.org/

3.4.5. Users may not connect unauthorized removable storage devices, such as USB thumb drives, cell phones or tablets, to county hardware unless they have been encrypted or approved by BCIT. A request for encryption can be placed in the BCIT ticketing system.

3.4.6. Users must report any weaknesses in computer security to the Information Security Team for follow-up investigation. If you see unusual system behavior such as random error messages about missing files, newly installed software or internet toolbars added unexpectedly, this could be a warning sign of malware infection. Please report suspicious or questionable system behavior via the BCIT Service Desk so your computer can be investigated.

3.4.7. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of Buncombe County proprietary information. Any workforce member who suspects that there has been an electronic or paper-based information breach must immediately report the situation to securityincident@buncombecounty.org. Please refer to the Buncombe County Information Breach Notification Policy.

3.4.8. Users must report any incidents of possible misuse or violation of the Acceptable Use Policy to their Supervisor. The supervisor shall contact securityincident@buncombecounty.org immediately and HR if deemed necessary.

3.4.9. Employees must complete security training that is automatically generated upon failing a phishing test. Phishing tests are conducted periodically and will prompt anyone who does not successfully report an opened and read phishing email.

3.5. **County Data**

3.5.1. BCIT Systems are subject to monitoring at any time, with or without notice, to verify that Buncombe County property is being used in a manner consistent with all county policies.

3.5.2. Accessing data, a server, or an account for any purpose other than conducting Buncombe County business, even if you have authorized access, is prohibited.

3.5.3. Users must always protect the integrity and confidentiality of non-public data. Extreme due care must be exercised when storing sensitive data. Sensitive data should not be saved to an internal or external hard drive. Do not extract sensitive information from an application and store in a location accessible to unauthorized users. Encrypted network storage systems provided by the County are to be used for storing all sensitive data.

3.5.4. Users are prohibited from downloading non-public data to personally owned devices.

3.5.5. Users must comply with the County's adopted Records Retention Guidelines. Documents are not allowed to be stored in a location not subject to central discoverability or record retention.

3.5.6. Users must not use or create accounts for unauthorized applications and cloud services such as, but not limited to, DropBox, Gmail, and Google Drive while conducting County business. It is permitted to receive information from other applications. Personal email accounts should not be used when conducting County business.

3.5.7. Users should avoid sending County data to non-authorized individuals, accounts, or services via an auto-forwarding capability. This prohibition extends to a user's personal email account. Forwarding of County email and data should follow the compliance measures outlined within this policy.

4. Policy Non-Compliance

Employees willfully violating the terms and conditions of this policy may be subject to appropriate disciplinary action, up to and including dismissal.

5. Audit

All policies for Buncombe County may be subject to audit or review as outlined in the Internal Auditor's Statement.

6. Definitions

6.1. Buncombe County Information Technology (BCIT) Systems - Any combination of computer software, computer hardware, telecommunications capabilities (including all voice, data and video networks) and/or other similar or related items of automated,

computerized, and/or software systems that are used or relied on by Buncombe County for operations.

6.2. Central Discoverability - Ability for ediscovery managers to search, audit, collect, compile data for the purpose of reporting or investigation. Software and network storage systems provided by BCIT are discoverable.

6.3. Computer Virus - A malicious computer program designed to interfere or harm normal daily computer operations.

6.4. County Data (Enterprise Data) - The totality of the digital information in the County. All digital information regarding clients, employees, and county business and/or operations.

6.5. Defacement - Altering the appearance of hardware by applying decals, graffiti, permanent fixtures, or modifications.

6.6. Denial of Service (DoS) - cyber-attack that makes network resources unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

6.7. Email - Distribution of messages, documents, files, software, or images by electronic means. This includes internal email, external email, and internet email.

6.8. Encryption - Encryption is the process of taking plain text, like a text message or email, and scrambling it into an unreadable format. This helps protect the confidentiality of digital data transmitted through a network like the internet.

6.9. Firewall - Used to prevent unauthorized access to Buncombe County's computer servers, networks, and clients while permitting outbound communications.

6.10. Hacking - The gaining of unauthorized access to data in a system or computer.

6.11. Internet - Global system of interconnected computer networks that allows users to communicate between networks and devices.

6.12. Mobile Device - a piece of portable electronic equipment that can connect to the internet, especially a smartphone or tablet computer.

6.13. Network Sniffing - the use of a software or hardware tool that monitors, snapshots or copies packets flowing over a computer network in real time without redirecting or altering that data.

6.14. Open-Source Software - A type of license for computer software that allows the application to be used, modified and/or shared under defined terms and conditions. Open-source licensed software is mostly available free of charge.

6.15. Packet (IP) Spoofing - the creation of Internet Protocol (IP) packets having a source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.

6.16. Personal Device - A privately owned device that may be used for a combination of personal and business use.

6.17. Phishing - type of email scam where messages appear to be from a legitime source that try to trick recipients into giving private information (i.e., username, password, account number, etc.)

6.18. Sensitive/Confidential data - Confidential or other regulated data protected by statute. Examples of regulated information include Criminal Justice Information (CJI), Health Insurance Portability and Accountability Act (HIPAA), Personal Health Information (PHI), other Personal Identifying Information (PII) and personnel information.

6.19. Software as a Service (SaaS) - Third-party, subscription-based software. Web-based software hosted by SaaS provider and commonly integrates with the county network. Buncombe County data stored in this SaaS software is owned by Buncombe County, however the application is only licensed on a subscription basis.

6.20. Streaming Content – Streaming refers to any media content – live or recorded – delivered to computers and mobile devices via the internet and played back in real time. Podcasts, webcasts, movies, TV shows and music videos are common forms of streaming content.

6.21. User - Individuals authorized to access the information technology resources of Buncombe County, including, but not limited to equipment, facilities, technologies and/or data. Users include Buncombe County employees, contractors, students, interns, volunteers, temporary staff, vendors and any other individual(s) or group authorized by the County to use or access resources.

7. Approval and Revision History

Policy Origination Date:	August 2, 2005
Requires Board Approval:	☐Yes ☒No
Board Approval Date:	Click for Date
Revision History	7/20/2005 – Original Document 9/7/2011 – Removed redundancies, updated technologies 9/13/2021 – updated technologies, streamlined language 10/22/2021 - corrected error in numbering at 3.4.6., edited annual acceptance wording 8/9/2024 – updated service desk link (p3, sec3.4.4)