1.0 Overview

Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the County network. This procedure explains how County information technology resources are to be used and specifies what actions are prohibited. While this procedure is as complete as possible, no procedure can cover every situation, and thus the user is asked additionally to use common sense when using County resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

2.0 Purpose

Since inappropriate use of County systems exposes Navajo County to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this procedure is to detail the acceptable use of County information technology resources for the protection of all parties involved.

3.0 Scope

The scope of this procedure includes any and all use of County IT resources, including but not limited to, computer systems, email, the network, and the County Internet connection.

4.0 Procedure

4.1 E-mail Use

Personal usage of Navajo County email systems is permitted as long as A) such usage does not negatively impact the County computer network, and B) such usage does not negatively impact the user's job performance.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered
Navajo County

<table>
<thead>
<tr>
<th>Acceptable Use Procedure</th>
<th>Created: 6/19/2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section of: County Security Procedures</td>
<td>Target Audience: Users, Technical</td>
</tr>
<tr>
<td>CONFIDENTIAL</td>
<td>Page 2 of 8</td>
</tr>
</tbody>
</table>

confidential or proprietary to Navajo County should not be sent via email, regardless of the recipient, without proper encryption.

- It is Navajo County procedure not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. At the time of this writing the acceptable file size is 10mg.

Please note that detailed information about the use of email may be covered in Navajo County's Email Procedure.

4.2 Confidentiality
Confidential data must not be A) shared or disclosed in any manner to non-employees of Navajo County, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other procedures may refer to the proper use of this information in more detail.

4.3 Network Access
The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access. If you notice that you have elevated access please notify the IT department.

4.4 Unacceptable Use
The following actions shall constitute unacceptable use of the County network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the County network and/or systems to:

- Engage in activity that is illegal under local, state, federal, or international law.
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to Navajo County.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.
- Install or distribute unlicensed or "pirated" software.
- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

### 4.5 Blogging and Social Networking

Blogging and social networking by Navajo County's employees are subject to the terms of this procedure, whether performed from the County network or from personal systems. Blogging and social networking is only allowed from the County computer network if it is required as part of the employee's job function. In no blog or website, including blogs or sites published from personal or public systems, shall Navajo County be identified, County business matters discussed, or material detrimental to Navajo County published unless directed by the Department head or as a function of the employees job function. The employee may identify himself or herself as an employee of Navajo County in a blog or on a social networking site but not as an official spokesperson of the County. The user assumes all risks associated with blogging and/or social networking. An example of an exception to this section is the use of the Navajo County Yammer network.

### 4.6 Instant Messaging

Instant messaging is allowed such that it follows guidelines on disclosure of confidential data and does not negatively impact the user's job function.

### 4.7 Overuse

Actions detrimental to the computer network or other County resources, or that negatively affect job performance are not permitted.

### 4.8 Web Browsing

The Internet is a network of interconnected computers of which Navajo County has very little control. The user should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. Navajo County is specifically not responsible for any information that the user views, reads, or downloads from the Internet.
Navajo County

Acceptable Use Procedure

<table>
<thead>
<tr>
<th>Section of: County Security Procedures</th>
<th>Target Audience: Users, Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIDENTIAL</td>
<td>Page 4 of 8</td>
</tr>
</tbody>
</table>

Personal Use. Navajo County recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of County computer systems to access the Internet is permitted as long as such usage follows pertinent guidelines elsewhere in this document, departmental procedures, and does not have a detrimental effect on Navajo County or on the user's job performance.

4.9 Copyright Infringement
Navajo County's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use procedure, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

4.10 Peer-to-Peer File Sharing
Peer-to-Peer (P2P) networking is not allowed on the County network unless it is part of their job function.

4.11 Streaming Media
Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media is allowed for job-related functions only.

4.12 Monitoring and Privacy
Users should expect no privacy when using the County network or County resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. Navajo County reserves the right to monitor any and all use of the computer network. To ensure compliance with County procedures this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.13 Bandwidth Usage
Excessive use of County bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low County-wide usage.
4.14 Personal Usage
Personal usage of County computer systems is permitted as long as such usage follows pertinent guidelines elsewhere in this document, departmental procedures, and does not have a detrimental effect on Navajo County or on the user's job performance.

4.15 Remote Desktop Access
Use of remote desktop software and/or services is allowable as long as it is provided by Navajo County. Remote access to the network must conform to Navajo County's Remote Access Procedure.

4.16 Circumvention of Security
Using County-owned or County-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

4.17 Use for Illegal Activities
No County-owned or County-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing
- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of Terrorism
- Identity Theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes
- Downloading, storing, or distributing illegally obtained copyrighted material

Navajo County may take all necessary steps to report and prosecute any violations of this
4.18 Non-County-Owned Equipment
Non-County-provided equipment is expressly prohibited on Navajo County’s network except for the public/secured internet unless approved by the IT Department.

4.19 Personal Storage Media
Personal storage devices represent a serious threat to data security and are expressly prohibited on Navajo County’s network unless approved by the IT Department.

4.20 Software Installation
No non-County-supplied software is to be installed without written permission of the IT Department. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. For these reasons, installation of non-County-supplied programs is strongly discouraged. If a certain program is required for his or her job function, the user should contact the IT Department to request permission.

4.21 Reporting of Security Incident
If a security incident or breach of any security procedures is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the Navajo County Incident Response Procedure. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains County information.
- Loss or theft of ID badge or keycard.
- Any attempt by any person to obtain a user’s password over the telephone or by email.
- Any other suspicious event that may impact Navajo County's information security.

Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

4.22 Third party systems on the Navajo County network

Acceptable Use Procedure

Confidential
There are many third party systems used on the Navajo County network and each of these systems should be updated regularly by the vendor that supplies the software/hardware. A maintenance contract should be in place for the systems supplied and only vendor supported software/hardware should be in operation on the Navajo County network unless approved by the IT Director. If a system does not have vendor support the IT staff will take steps to isolate these systems to mitigate the possibility of security risks. This may include isolating segments of the network, installation of internal firewalls or limiting access in other ways. The ways that this isolation is achieved will change and will be determined by the IT staff to insure the safety of the network.

4.23 Applicability of Other Procedures
This document is part of Navajo County’s cohesive set of security procedures. Other procedures may apply to the topics covered in this document and as such the applicable procedures should be reviewed as needed.

5.0 Enforcement
This procedure will be enforced by the IT Director and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of County property (physical or intellectual) are suspected, Navajo County may report such activities to the applicable authorities.

6.0 Definitions

**Blogging** – The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

**Instant Messaging** – A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

**Peer-to-Peer (P2P) File Sharing** – A distributed network of users who share files by directly connecting to the users’ computers over the Internet rather than through a central server.

**Remote Desktop Access** – Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.
Streaming Media – Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

7.0 Revision History

Revision 1.0, 6/19/2015
Revision 1.5, 9/23/2015
Revision 1.6, 1/20/2016
Revision 2.0, 05/25/2016