Section 4: Professional Workplace

Policy #4: Use of Technological Resources
Effective Date: January 1, 2018

I. Purpose

The purpose of this policy is to educate each employee as to what is acceptable and unacceptable usage of the Town's technological resources. The Town of Mooresville provides Information Technology resources as tools to help each employee carry out their functions for the Town.

II. Scope

This policy shall apply to all persons holding a paid position as an employee of the Town, except the Town Manager, Town Attorney, a member of any appointed or volunteer board or committee, or any others that may be excluded by the Town Board. For this purpose, and subject to the exceptions set out herein, Town employees shall be defined as those employees in departments and offices for which the Town Board serves as the final budget authority.

III. Background

None

IV. Definitions

Information Technology Resources – includes but is not limited to: office phones, cell phones, facsimile machines, copier machines, computers, laptops, the Internet, hardware, software, and data.

V. Legislation

None

VI. Policy

It is the policy of the Town that all employees shall use Town owned, operated, leased, and maintained technology resources in an appropriate manner.

VII. Provisions

A. E-Mail usage
   i. All E-Mail will be archived for a period of two years.
   ii. Messages sent or received may be public records.
   iii. Frequent deletion of old and unneeded email is the responsibility of each user.

iv. Use of the "All User" distribution list is restricted to the Mayor, Town Manager's office, Department Directors and their specific designees.
v. Sending or forwarding emails that are inappropriate or offensive is not permitted.
vi. Employees must use caution when opening email attachments or clicking on hyperlinks as these may contain viruses or malware capable of damaging Town data.
vii. Employees should refrain from the use of removable media devices (thumb drives, portable hard drives, CD/DVDs) to store personally identifiable or criminal justice information unless steps are taken to encrypt such storage devices.

B. Remote Access Policy
i. It is the responsibility of employees when using personally owned equipment to connect to the Town networks via VPN, to ensure their devices are running up to date anti-virus software along with updated operating systems.
ii. Remote Access will be strictly controlled and reviewed regularly to ensure access is removed when no longer required.
iii. Authorized users are responsible for maintaining control of security tokens, passwords, and PINs related to remote access capabilities.
iv. Vendor accounts with access to the Town network will only be enabled during the time period access is required and will be disabled or removed once access is no longer needed.

C. Passwords
i. A password shall be composed of eight (8) characters combining three (3) of the four (4) following characters: upper case letter, lower case letter, number, or symbol.
ii. The life of a password shall not exceed 90 days.
iii. A user's account shall be locked for at least 30 minutes if there are at least five (5) successive invalid entries of a password, unless a helpdesk ticket is submitted to unlock the user account.
iv. Any password shall be considered confidential information and must not be shared. Any action taken with an employee's credentials is the sole responsibility of the user that the credential is issued to.
v. If there is any doubt about the confidentiality of a password, the password should be changed.
vi. Screen Savers will become active after 15 minutes of non-use. The screen saver will become password protected when returning to normal state.

D. Cell Phones

i. There will be no personal phone calls made or accepted using Town issued cell phones.
ii. All department directors and supervisors will be allowed a data/cell phone upon approval of the immediate supervisor.
iii. All other Town cell phone requests must be approved by the Department Director and Town Manager.
iv. All communication systems' invoices will be randomly audited by the Finance Department.
v. If a phone needs to be replaced due to negligence (lost, dropped, wet), a replacement must be approved by the Department Director and Town Manager. Employee may be held financially responsible for repeated loss or damage of a cell phone.

E. Social Networking

If your Department participates in social media, follow these guiding principles:

i. Ensure that the Public Information department is aware of your official participation and representation on social media sites, including giving IT admin privileges to each site.
ii. Stick to your area of expertise and provide unique, individual perspectives on what is going on in the Town.
iii. Post meaningful, respectful comments, no spam, and no remarks that are off-topic or offensive.
iv. Pause and think before posting. Reply to comments in a timely manner, when a response is appropriate.
v. Respect proprietary information, content, and confidentiality.
vi. When disagreeing with others' opinions, keep it appropriate and polite.
vii. Please recognize the difference between social media as a private individual and social media as a public or government representative.
viii. Make sure your efforts to be transparent do not violate the State's privacy, confidentiality, and any applicable legal guidelines for external communication.

F. Unacceptable Uses of Information/Technological Resources

The following are examples of unacceptable uses for Town of Mooresville informational and technological resources:

i. Conducting the operations of a business other than Town of Mooresville business.
ii. Using the Internet to gamble in any form.
iii. Accessing, storing, or transmitting offensive material.
iv. Any attempt to harm, modify, or destroy computer hardware or data of another user, the Internet, or any other networks associated with the Town.
v. Disruption or unauthorized monitoring of electronic communications.

G. Unauthorized Uses of Information Technology Resources
   i. Taking Town of Mooresville hardware out of the office, including, but not limited to computers, workstations, servers, etc. (Laptops are assumed to be taken out of the office for Town business use.)
   ii. Changing or tampering with hardware on a Town of Mooresville computer, workstation, server, laptop, or any other device connected to the Town of Mooresville network.
   iii. Reverse engineering or disassembling any hardware.
   iv. Attempting to circumvent security or access control mechanisms.
   v. Adding any unauthorized device to the Town of Mooresville network such as cell phones, personal laptops, personal printers, etc. Employees are allowed to connect any personal device to the Town of Mooresville guest wireless network.

H. Miscellaneous
   i. This policy may be updated at any time to be current with new technology.
   ii. The Town reserves the right to monitor, record, and audit communications occurring on the Town of Mooresville Network including but not limited to email and internet access. Requests for inspection and monitoring of employee usage must be requested by the Department Director, approved by the Town Manager, in conjunction with the IT Director.
   iii. Tools used to inspect and monitor usage are in place to be used at the request of Department Directors. In no way will the IT department be responsible for policing such usage.
   iv. Any violations of this policy may subject an employee to disciplinary action up to and including termination.

VIII. Authorization

Approved by:

David Treme — Town Manager

01/02/2018 — Date