



**TOWN OF BLACK MOUNTAIN
EMPLOYEE COMPUTER, E-MAIL, INTERNET and SOCIAL MEDIA USAGE POLICY**

I. OVERVIEW

This document constitutes a Town-wide policy intended to outline the proper use of all Town of Black Mountain computer and network resources, the effective protection of individual employees, and proper management of those resources. These guidelines are intended to supplement, not replace, any and all existing laws, regulations, policies, agreements, and contracts which may apply to these resources.

Employees' access to computers and network resources owned or operated by the Town of Black Mountain impose certain responsibilities and obligations and is granted subject to relevant Town policies and local, State and Federal laws. Appropriate use should always be legal and ethical for the furtherance of the Town's mission and goals and to reflect community values, uphold the Town's reputation, maintain public confidence in the Town organization and show restraint in the consumption of shared resources.

The policy also addresses the use of various forms of social media by Town employees, either with Town computer and network resources or their own personal computer and network resources, to insure that such usage is not detrimental to other Town employees or the Town organization.

II. EMPLOYEE RESPONSIBILITIES AND RIGHTS

- **Use of resources**

Town computer, e-mail, network, and internet resources are provided to assist the employee in performing assigned work in an efficient and effective manner for the benefit of the citizens of the Town of Black Mountain. These resources should be used for official Town business only, with the exception of incidental personal use outlined in Section VI of this policy.

- **Privacy**

To the greatest extent possible in a public setting, the Town seeks to preserve the employee's privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, users must recognize that Town computer and network resources are public, the property of the Town of Black Mountain, and as such may be subject to review under the North Carolina Open Records Act, and are subject to periodic review by authorized Town personnel. Employees should utilize such systems at their

own risk, and with the awareness that Town computers and network resources are not to be treated in the same way as one's personal computer and network resources.

- **Freedom of Expression**

The constitutional right to freedom of speech applies to all employees of the Town no matter the medium used; however, Town employees are liable and accountable for all works and forms of expression exhibited during the performance of official Town duties. Thus, in accordance with this policy, Town employees should recognize the difference between freedom of expression as a general citizen and freedom of expression as a public employee of the Town of Black Mountain.

- **Ownership of data and information**

All forms of data either stored on or transmitted to or from Town computers using the Town's network resources are the property of the Town of Black Mountain.

- **Freedom from harassment and undesired information**

All employees have the right not to be harassed by computer or network usage by others.

- **Common courtesy and respect for rights of others**

Each employee is responsible for respecting and valuing the rights of privacy for all, to recognizing and respecting the diversity of the population and opinions in the community. Each employee must behave ethically, and comply with all legal restrictions regarding the use of information that is the property of others.

- **Privacy of information**

Files of personal information, including programs, no matter on what medium they are stored or transmitted, may be subject to the North Carolina Open Records Act if stored on Town computers or network resources. That fact notwithstanding, no one should look at, copy, alter, or destroy another individual's personal files without explicit permission (unless authorized or required to do so by law or regulation). Simply being able to access a file or other information does not imply permission to do so.

- **Harassment**

No employee of the Town may, under any circumstances, use Town computers and network resources to libel, slander or harass any other person. The following shall constitute computer harassment:

1. Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family.
2. Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease.
3. Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

- **Information integrity**

It is the employee's responsibility to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable

nature of electronically stored information, and to verify the integrity and completeness of information that the employees compile or uses.

- **Responsibility for security, maintenance, and proper care of assigned computer resources**

Each employee is responsible, in coordination with the employee's department director, for the security and integrity of Town information stored on Town computers assigned to the employee. This responsibility includes controlling physical and network access to the machine, and using the supplied virus protection software. Employees must not write down or otherwise store passwords or other information that can be used to gain access to other Town computing resources, unless the access information is stored in a secured place and not accessible to others.

- **Virus Detection**

Files obtained from sources outside the Town's network including storage devices brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage the Town's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use devices from non-Town sources, without first scanning the material with the Town-approved virus checking software. If you suspect that a virus has been introduced into the Town's network, notify your supervisor immediately.

III. E-MAIL AND OTHER ELECTRONIC COMMUNICATIONS

Electronic communication systems provide a useful way to exchange ideas, share files, and maintain relationships with colleagues, and are a valuable asset. Messages sent and received through the Town network, email, the Internet, and social media sites (including notes, memos, purchase orders, letters, and other documents, created on Town computers and network resources) are the property of the Town.

Messages and files, like other types of correspondence and Town documents can be accessed and read by authorized Town personnel and may be subject to the North Carolina Open Records Act. Authorized access to employee's electronic communications by other employees or authorized individual includes, but is not limited to, the following:

- Access by Information Technology staff during the course of system maintenance or administration.
- Access approved by the employee, the employee's supervisor, or the Town Manager when there is an urgent need to access the employee's mailbox or other computer files.
- Access approved by the employee's supervisor and the Town Manager when there is reason to believe the employee is using the communication system in violation of the Town's policy, and
- Access approved by the Town's legal counsel in response to the Town's receipt to a court order or request from law enforcement officials for disclosure of an employee's email messages.

The Town's computer and network resources should not be used to communicate sensitive or confidential information. Employees should appreciate that an electronic message might be disclosed to or read by individuals other than the intended recipient(s), since the message

can easily be forwarded to other individuals. In addition, while the Town endeavors to maintain the reliability of its electronic communication system, employees should be aware that a variety of human and system errors have the potential to cause inadvertent or accidental disclosure of electronic messages.

- **No expectation of privacy**

Employees are provided with computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, send, or receive using the Town's computer equipment and should consider all data contained on a Town machine as Public Record. The computer network is the property of the Town and may be used only for the Town's purposes. Additionally, any Town information files or e-mails that are on an employee's home computer, smart phone, tablet or other device must be considered Public Domain and is discoverable if requested by certain entities for legal purposes.

IV. USE OF THE INTERNET

The Town of Black Mountain provides access to the vast information resources of the internet to help employees perform their work in an efficient and effective manner. The Town's facilities that provide access to the internet represent a considerable commitment of resources for telecommunications, networking, software, storage, etc. Town's computing and network resources are provided for Town employees for official Town business activities only, with the exception of incidental personal use outlined in Section VI of this policy.

All existing Town personnel policies apply to employee conduct on the internet, especially (but not exclusively) those that deal with employee performance, personal conduct, intellectual property protection, privacy, misuse of Town resources, sexual harassment, information and data security, and confidentiality. Employees must conduct themselves honestly and appropriately on the internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others. Unlawful or inappropriate internet usage may garner negative publicity for the Town and expose the Town to significant legal liabilities.

- **Monitoring of computer and internet usage**

The Town has the right to monitor and log any and all aspects of its computer system including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups and social networking sites, monitoring file downloads, and all communications sent and received by users.

V. SOCIAL MEDIA

While the Town encourages its employees to enjoy and make productive use of their personal time, certain activities on the part of employees may become a concern if they have the effect of impairing the work of any employee, harassing, demeaning, or creating a hostile working environment for any employee, disrupting the smooth and orderly flow of work within the organization, harming the goodwill and reputation of the Town among its citizens, or eroding public confidence in the Town organization.

In the area of social media (print, broadcast, digital, blogs, personal websites, and online services such as Facebook, LinkedIn, MySpace, Plaxo, Twitter, news media comment boards, and others), employees may use such media in any way they choose as long as such use does

not produce the adverse consequences noted above for the Town. For this reason, the Town of Black Mountain reminds its employees that the following guidelines apply in their use of social media on their own personal time and personal computer resources as well as work time.

If an employee publishes any personal information about the employee, another employee of the Town, the organization, a citizen, or a customer in any public medium (print, broadcast, digital, or online) that:

- Has the potential effect of involving the employee, their coworkers, or the Town in any kind of dispute or conflict with other employees or third parties.
- Interferes with the work of any employee.
- Creates a harassing, demeaning, or hostile working environment for any employee.
- Disrupts the smooth and orderly flow of work, or the delivery of services to the Town's citizens.
- Harms the goodwill and reputation of the Town among its citizens or in the community at large.
- Erodes the public's confidence in the Town organization, or
- Tends to place in doubt the reliability, trustworthiness, or sound judgment of the person who is the originator or subject of the information, then

the employee(s) responsible for such problems will be subject to counseling and/or disciplinary action, up to and potentially including termination of employment, depending upon the severity and repeat nature of the offense.

Employees who conduct themselves in such a way that their actions toward and relationships with each other interfere with or damage work relationships, disrupt the flow of work or customer relations, or cause unfavorable publicity in the community, should be concerned that their conduct may be inconsistent with one or more of the above guidelines. In such a situation, the employees involved should request guidance from their supervisor to discuss the possibility of a resolution that would avoid such problems. Depending upon the circumstances, failure to seek such guidance may be considered evidence of intent to conceal a violation of the policy and to hinder an investigation into the matter.

Use of social media that involves any kind of criminal activity or harms the rights of others may result in criminal prosecution or civil liability to those harmed, or both.

Social Media access and use involving Town equipment and resources are subject to the Town of Black Mountain Computer, Network, E-mail, and Internet Usage Policy at all times.

How an employee uses social media is not a matter of concern as long as it is consistent with the above guidelines. Employees may address any questions on this policy to their Department Directors.

VI. PERSONAL USE OF TOWN COMPUTER AND NETWORK RESOURCES

Town computer facilities, services, and networks may not be used in connection with compensated outside work or for the benefit of individuals or organizations not related to the Town of Black Mountain, except in connection with official Town activities (such as employees publishing public and employee activities). Town computers and network resources may not be used to view sexually explicit or inappropriate materials.

Incidental and short duration personal use of Town computers and network resources, including access to the internet, is authorized, provided such use occurs on the employee's own time (i.e. during lunch time) and such use is legal, ethical, reflects community values, does not compromise the Town's reputation or the public's confidence in the Town organization and does not compromise the Town's networks, systems or this usage policy.

Any incidental use (such as electronic communications or storing data on single user machines) must not interfere with other users' access to resources (computer cycles, network bandwidth, disk space, printers, etc.) and must not be excessive.

If users receive unsolicited email from outside the Town that appears to violate this policy, the user should notify his or her supervisor immediately. Similarly, if any user accidentally accesses an inappropriate website in the normal course of business, the user should notify his or her supervisor immediately.

VII. DEPARTMENT DIRECTOR/SUPERVISOR RESPONSIBILITY

It is the responsibility of the Department Directors and Supervisors to support and administer this policy and to ensure employee knowledge of, and compliance with, the principles outlined in this policy. In addition, it is the responsibility of Department Directors to develop, inform and administer any additional policies/protocols regarding the transmittal of confidential or otherwise sensitive information specific to their department's operations.



EMPLOYEE CONSENT FORM

Employee Name: _____

I, the above-named employee of the Town of Black Mountain, have read this policy and agree to comply with all its terms and conditions. I agree that all computer and network activity conducted while doing business on behalf of the Town of Black Mountain and being conducted with Town resources is the property of the Town of Black Mountain.

The Town of Black Mountain reserves the right to monitor and log all computer and network activity including e-mail and other electronic communications, with or without notice, and therefore users should have no expectations of privacy in the use of these resources.

I understand that violations of this policy may result in disciplinary action, up to and including termination of employment and/or legal action.

Signed: _____

Date: _____

Supervisor: _____

Date: _____