TOWN OF BLOOMFIELD

POLICY MEMORANDUM

SUBJECT:	IT Department's Internal Policies & Procedures	NO:	146.02
		DATE:	8/20/2013
		AMENDED:	
DISTRIBUTION:	All Departments	BY:	Sandy Rosenberg, Director of Information Systems and Technology
		APPROVED:	

I. PURPOSE

This document establishes guidelines to be used by the Information Systems and Technology Department (IT) personnel. These guidelines are intended to help IT personnel carry out their duties efficiently and effectively and to protect the rights and privacy of Town technology users as well as those of the IT personnel themselves.

II. RESPONSIBILITY

Individuals employed in the Information Systems Department are subject to these policies.

III. FORMS

None

IV. PROCEDURE

A. ADHERENCE TO LAWS AND TOWN POLICIES

i. In carrying out their assigned duties, IT personnel will adhere to all Federal, State and Local laws.
ii. This policy does not replace the Town Computer and Internet Use policy provided in the employee manual.
iii. All technology users will be treated with patience and respect.
iv. IT staff will not install or support any software that is not properly licensed.

B. SPECIAL ACCESS

i. In order to adequately support the IT needs of the Town, IT personnel have access to most offices where computing equipment is in use. The keys to these offices should never be used

for any purpose other than carrying out IT duties or for giving access to the members of the Department in question.

ii. Department Heads should be notified in advance of all planned access to other departments outside of normal working hours. If access is needed due to an emergency, the department heads should be notified as soon as possible.

iii. IT personnel have privileged access to on-line files and information. This access should never be shared with anyone outside IT unless authorized by the department that owns the data, and this access should never be used for any purpose other than the performance of IT duties.

iv. IT personnel should not provide access to data to another user unless authorized to do so by the head of the department that owns the data.

v. IT personnel have the ability to create user accounts and give users access to data. No account should be created or data access granted without a written or e-mailed request from the employee's supervisor or designated personnel or the owner of the data.

C. PRIVACY OF DATA/INFORMATION

i. When assisting users, IT staff may use, discuss and/or disseminate the User's data/information only to the extent necessary to perform the work required to assist them. Particular emphasis should be placed on restricting disclosure of the data/information to those persons who have a definite need for the data in order to perform their work.

ii. IT staff will not reproduce the User's data/information (except in the course of routine backups) unless authorized to do so by the IT Director or the head of the department which owns the data.

iii. IT Staff will not discuss and/or disseminate a User's data/information to third parties unless authorized to do so by the IT Director or the head of the department that owns the data.

D. RECORD KEEPING

i. Service Requests: Whenever a request for service is received, a ticket should be opened in Qalert (or whatever tracking software is currently in use). Actions taken should be logged, and the ticket should be closed promptly when the issue has been resolved. Anything that requires more than a minute or two should be logged.

ii. Problem originators should be kept informed of the status of the problem and any actions taken to ameliorate it.

iii. Any service request that occurs outside of normal working hours and results in comp time accrual must be logged. No comp time accrual will be approved without a corresponding entry in the service request log. Except in the case of an emergency, all comp time must be approved by the Director of Information Systems and Technology.

iv. When a new employee comes on board, his or her department head must request set up of an account and specify what programs the employee should have access to. This request should be in writing or via e-mail. There are checklists located in the \IT\Policies\forms directory

that specify the tasks needed for a new employee. A new instance of the checklist should be created for each new hire that receives computer accounts, and the checklists should be stored on-line.

v. The IT Department should be informed by the HR Department when any employee is terminated for any reason. Termination checklists are located in the \IT\forms directory, and a new one should be filled out for each terminating employee with a computer account. The checklist should be stored on-line.

vi. Equipment Deployment - Configuring a new PC for a user has many steps. To assure that none are missed, employees must use a checklist located in the \IT\Policies\Forms directory. A copy of the checklist should be made for each new deployment and the completed form should be stored on-line.

E. INAPPROPRIATE USE

i. If an IT staff member has reason to suspect that an employee is using Town computer equipment inappropriately, he or she should report it to the IT Director. Inappropriate use is clearly defined in the Internet and Computer Use policy found in the Employee Handbook. The IT Director will examine the evidence. If there is misconduct, the IT Director will report it to the HR Department.

ii. In the event that an employee intentionally commits an act that damages or endangers the functioning and or content of Town servers, immediate steps should be taken to remove the employee's access to the Town computing equipment.

F. PRIORITIES

The IT department often has many open problem tickets. In choosing which problem to attend to, the highest priority is the one that prevents the most employees from performing their duties. Thus, problems with the servers or network always get the highest priorities. Next priority would go to problems that prevent an employee from carrying out his or her assigned duties. In the event of total PC failure, the IT Department will make every effort to remedy the situation as quickly as possible.

APPENDIX A
AGREEMENT FOR IT PERSONNEL

I certify that I have received, read and understood the IT Department's Policies and Procedures, as described above, and will comply with the conditions within it.

Name	Department
Signature	Date