Town of Ponce Inlet

4300 South Atlantic Avenue, Ponce Inlet, FL 32127
ph: 386-236-2150

Computer Policy 2008

Town of Ponce Inlet

Information Technology and Computer Usage Policies

May 21, 2008

1.0 Governance Policy

1.1 Policy

The mission of the Technology function is to provide cost effective computing tools to the employees of the Town of Ponce Inlet (Town) in order to facilitate their ability to effectively and efficiently serve the customers and residents of the Town. The Technology function is just that, an overall function, with the operational component of the Technology function being the Town's IT Manager. Internal (IT Manager) and external (JBT) service providers make up the Technology function.

1.2 Management and Organization

The Technology function reports to the Town Manager.

2.0 Computer Hardware

2.1 Policy

All computer hardware purchased for use within the Town, whether on the network or not, shall be purchased and installed by the Technology function. The Town will not purchase computer hardware until the resources are available to install the equipment.

2.2 Purpose/Description

Having the Technology function purchase and install computer hardware will ensure the hardware purchased conforms to Town technical standards, meets computer security requirements and interfaces properly with other computerized equipment.

2.3 Enforcement

Purchasing will reject all requests for computer hardware that are not approved through the IT Manager. Any computer hardware found to be in use without the IT Manager approval will be disconnected immediately and confiscated. The incident will be reported to the violator's Department Head and the Town Manager and may result in disciplinary action.

2.4 Responsibilities

IT Manager – Purchases and installs all computer hardware. The IT Manager will maintain and periodically inventory all hardware within the Town to confirm policy enforcement and to provide for verification of fixed asset tracking for insurance purposes.

Purchasing – Ensures that all requests for computer hardware are generated by the IT Manager.
Employee – Work with the Technology function to determine hardware needs and to develop an appropriate annual budget.

Department Heads – Ensure enforcement of the policies through disciplinary actions as necessary against those violating the policy.

3.0 Computer Software

3.1 Policy

All computer software purchased for use within the Town, whether on the network or not, shall be purchased and installed by the Technology function. The Technology function will also provide for the maintenance of any packaged software and upgrade that software as needed. This policy applies to all operating system software as well as application software. The Town will not purchase computer software until the resources are available to install the equipment.

3.2 Purpose/Description

Having the Technology function purchase and install computer software will ensure the software purchased conforms to Town technical standards, meets computer security requirements and interfaces properly with other computerized hardware and/or software within the Town.

3.3 Software Acquisition

It is the policy of the Town to always purchase packaged software unless an overwhelming business need demonstrates the need to create a custom package. The Technology function does not have the resources to develop or maintain custom software packages.

Any packaged software purchases will allow escrowing of software source code to protect the Town in the event software vendor goes out of business.

All software packages will be purchased with software maintenance agreements that will be maintained by the Technology function.

Acquiring software to satisfy functional application needs is a joint responsibility between the Technology function and the employee's department. The employee's department is responsible for ensuring the software obtained meets its functional need. The Technology function will ensure the software can technically operate in the Town's environment and provide cost and budget information input into the decision-making process.

3.4 Software Responsibilities

The Technology function is responsible for ensuring the maintenance of software products through the applications of applying patches, upgrades and fixes. The Technology function will ensure the software is operational.

The employee's department is responsible for functional training and understanding how the software functionally operates to satisfy the business need.

3.5 Enforcement

Purchasing will reject all requests for computer software that do not originate from the Technology function. The IT Manager will provide written verification to the purchasing agent supporting the acquisition of any software used on the town's network or town client computer. Any computer software found to be in use without the Technology function approval will be removed immediately and confiscated. The incident will be reported to the violator's Department Head and the Town Manager and may result in disciplinary action.

3.6 Responsibilities

Employee's Department – Works with the Technology function to determine functional software requirements. Participates as an equal partner in the acquisition process. After purchase, the employee is responsible for understanding the functional aspects of the software and providing adequate end-user training on its use.
Technology Function – Works with employee as an equal partner in the acquisition process. Maintains the software in an operational state. Provides for updates and upgrades of the software in cooperation with the employee as new releases are issued.

Purchasing – Ensures that all requests for computer software are generated by the Technology function. Follows standard Town purchasing policies.

Department Heads – Ensure enforcement of the policies through disciplinary actions as necessary against those violating the policy.

4.0 E-Mail

4.1 Policy

As a productivity enhancement tool, the Town encourages the business use of e-mail. E-Mail access will be granted to all Town employees with computer technology capable of executing the programs unless specifically denied by the employee's Department Head.

4.2 Purpose/Description

The purpose of this policy is to clearly determine the acceptable uses of the Town's e-mail system and what actions are prohibited.

4.3 Ownership of the E-Mail System

The e-mail system belongs to the Town and the contents of any individual employee's e-mails may be accessed at anytime, with or without advance notice. While employees may have a personal password, the Town, without the employee's knowledge or consent, may access e-mail on the Town's e-mail system. Nothing in or on the e-mail system should be considered confidential.

4.4 Acceptable Use

Use of the Town's e-mail system is intended for Town related business. Communication by e-mail is encouraged when it results in the most efficient and/or effective means of communication. All employees are to use e-mail as they would any other type of official Town communications tool. When any e-mail is transmitted, both the reader and sender should consider if the communication falls within ethical guidelines.

Incidental and occasional personal use of the e-mail systems will be tolerated, but these e-mail messages will be treated the same as business related e-mail messages – with no expectation of personal privacy. Personal e-mails of a sensitive nature should not be sent using the Town's e-mail system. The following are additional guidelines to be considered when using the Town's e-mail system for personal use:

- Personal incoming or outgoing e-mail must be kept to a minimum so that it does not consume more than a trivial amount of system resources
- Personal incoming or outgoing e-mail must not interfere with an employee's work during working hours
- All personal e-mails must conform to the following sub-section on prohibited uses

4.5 Prohibited Uses

- The Town's e-mail system may not be used to promote or increase awareness of charities or fundraising campaigns unless those campaigns have been specifically approved in advance by the Town Manager
- E-Mail may not be used for soliciting or proselytizing commercial ventures, job searches, chain letters, religious or personal causes or other similar, non-job-related solicitations
- Employees may not use the Town's e-mail system in any way that might be seen as insulting, disruptive or offensive by other persons, or harmful to morale. Examples of such forbidden transmissions include sexually-explicit messages, gambling, cartoons or jokes, unwelcome propositions or love letters, ethnic or racial slurs or any other message that could be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, religion or political beliefs.

- Do not use the Town's e-mail system to send copies of documents that are in violation of copyright laws

- Do not use the Town's e-mail system to compromise the integrity of the Town or its business in any way

- The use of web-based e-mail for either personal or business related usage is strongly discouraged as this method of sending/receiving e-mail bypasses the Town's security perimeter and virus scanning tiers. It is strongly suggested that all e-mail must be sent and received by the client-side Outlook e-mail application.

- Use of e-mail to offer for sale non-Town related items

- The following disclaimer will appear on all outgoing emails…

PLEASE NOTE: Florida has very broad public records laws. Most written communication to or from Town of Ponce Inlet officials and employees regarding public business are public records available to the public and media upon request. Your e-mail communications may be subject to public disclosure. Under Florida law, e-mail addresses are public records. If you do not want your e-mail address released in response to a public records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing.

4.6 Retention of E-Mail

Each mailbox will have a mailbox limit that will not be expanded without the permission of the IT Manager. Mailbox limits are necessary to ensure the integrity of the entire e-mail system. When a user's mailbox is full, no more e-mails will be accepted for that user; and the sender will receive a notice that the e-mail cannot be delivered.

Users wanting to keep e-mails for a long period of time should remove them to an off-network storage area. Although the Technology function provides limited backup of e-mail, it is intended for system restoration purposes only. It is not designed to retain documents for public record purposes or long term storage. Town employees should set up their own electronic retention procedures to ensure that e-mails that are subject to public record requirements are properly retained.

4.7 Enforcement

The Technology function will provide for the enforcement of these policies through the use of monitoring technology. It will report violations to the Director of Administration, the Town Manager and the Department Head of the offending employee. Misuse may result in disciplinary action.

4.8 Responsibilities

Departmental Supervisors – Shall be held responsible for ongoing enforcement of this policy for employees under their control.

End-User – Shall be made aware of these policies and held accountable.

Department Heads – Ensure enforcement of the policies through disciplinary actions, as necessary, against those violating the policy.

Technology Function – Monitors e-mail system use and reports violations.

5.0 Internet

5.1 Policy

The purpose of this policy is to clearly define the acceptable use of the Internet and what actions are prohibited.

5.2 Purpose and Description

As a productivity enhancement tool, the Town encourages the business use of the Internet. Internet access will be granted to all Town employees with computer technology capable of executing the programs unless specifically denied by the employee's Department Head.

5.3 Acceptable Use

Use of the Town's Internet access is intended for Town related business. All employees are to use the Internet as they would any other type of official Town tool. Employees should consider ethical guidelines.

Incidental and occasional use of the Town's Internet system for personal reasons is permitted by Town employees but should follow ethical guidelines when using the Town's Internet system for personal use:

- Personal use must be kept to a minimum so that it does not consume more than a trivial amount of system resources
- Personal use must not interfere with an employee's work during working hours
- Employees should have no expectation of privacy when using the Town's Internet system
- All personal Internet usage must conform to the following sub-section with regard to prohibited uses

5.4 Prohibited Uses

Any use of the Internet to aid in "moonlighting" job searching, soliciting or proselytizing for commercial ventures, gambling, religious or personal causes or outside organizations, or for other similar non-job related solicitations is strictly prohibited. Use of the Town's Internet to access any Web site or material that is sexually explicit, pornographic or obscene or that could be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin or their religious or political beliefs is strictly prohibited.

Any use of the Town's Internet that might have the potential to cause the Town public harm or to cause damage to the Town's reputation is strictly prohibited.

Employees are prohibited from installing any browser plug-in or "enhancement applications" such as Flash, Real Media, Quick Time, Shock Wave, browser toolbars. This includes but is not limited to pop-up blockers, anti-spyware programs, screen savers, background changers or any other item that is not provided by the Technology function as part of the original system configuration or added at a later time by the Technology function.

5.5 Security and Blocked Access

The Technology function will provide for Internet security that includes but is not limited to firewall protection, specific routing, profiles and passwords. Specific web sites that have no legitimate business purpose will be blocked from access; these will include radio, television, entertainment and sexually explicit sites. Those with legitimate business need for accessing such sites should request exemption from their Department Heads and the Technology function. An audit trail of access to web sites will be maintained by the Technology function to investigate possible violation of Town policy or breaches in security. The fact that a web site is not blocked by the Technology function does not mean it is acceptable to the Town. Any web site, whether it is blocked or not, that falls within the prohibited use parameters is prohibited.

5.6 Public Representation

No media advertisement, Internet page, electronic bulletin board posting, electronic mail message, or any other public representation about the Town may be issued using the Town's computer equipment unless appropriate management has granted approval.

5.7 Enforcement

The Technology function will monitor Internet access through the use of technology tools. Violations will be reported to the Director of Administration, Town Manager and the Department Head of the offending employee. Misuse may result in disciplinary action.

5.8 Responsibilities

Departmental Supervisors – Share responsibility for ongoing enforcement of this policy for employees under their control.

End-Users – Must be made aware of these policies to ensure compliance.

Department Heads – Provide disciplinary action for those violating the policy.

6.0 Access to Computer/Network Systems

6.1 Policy

It is the policy of the Town to grant access only to systems and programs that are required in the performance of an employee's job. Temporary access will be granted to individuals when filling in for someone who is on vacation on another leave of absence. Department Heads will authorize access to systems and software under their control.

6.2 Purpose/Description

The purpose of this policy is to ensure that individuals only have access to the software and systems that are required to perform their duties. Restricting access in this manner minimizes the risk of both internal and external security violations.

Use of VPN (Virtual Private Network) access to the Town Network will be limited to those demonstrating need. VPN access will be granted only after prior approval of the IT Manager. VPN profiles and passwords shall not be copied by employees or shared.

The Technology function will be notified prior to an outside party (technology contractor/consultant) accessing the Town network via a VPN connection.

6.3 Enforcement

Access authorization documentation will be generated for each individual. This documentation will indicate what software and/or systems are to be accessed and what privileges (read, write, etc) are permitted. The Technology function will ensure that only the appropriate rights and privileges are granted to each the employee. Annually, the Technology function will review the rights and privileges of all individuals and provide a list to Department Heads for confirmation. Incidents of unauthorized access will be reported to the violator's Department Head and the Town Manager and may result in disciplinary action. Employee VPN privileges will be revoked if unauthorized VPN use is discovered.

6.4 Responsibilities

Technology Function – Grants rights and privileges for system access based upon a written authorization document that has been approved by an authorized individual. Annually produces a report of all individual rights and privileges and forwards the report to Department Heads.

Department Heads – Provide written documentation that authorizes access rights and privileges for each employee. Annually review and reconfirm accuracy of access rights and privileges.

Department Heads – Provide disciplinary action for those violating the policy.

7.0 Password Security

7.1 Policy

All Town computer systems are protected by individual user identification (UID) names and passwords. Town computer systems will track history by UID and password. History records will show who accessed (or attempted to access) what systems and when.

It is the responsibility of the individual user to protect his/her password as they would any other identification number such as their social security number or a credit card number.

It is a violation of this policy for an individual user to give his/her UID and/or password to any other individual within or outside the Town. It is a violation of this policy to write the password down and leave in an easy-to-find location.

7.2 Purpose/Description

All Town computer systems are UID and password protected to identify who is using the system and to limit to those rights and privileges they have within the system.

7.3 Password Make-Up and Expirations

Passwords will be complex, meaning they will have a minimum of 8 characters and must contain numbers and alphabetic and certain special characters. All passwords will expire on a 90-day basis. Employees may not reuse a password that has been used within the last year (the system will prevent this). This is required by best practice computer security standards.

Only the IT Manager has the authority to grant exceptions.

7.4 Enforcement

The Technology function will monitor the use of UID names and passwords to ensure only authorized users are able to access the system. The Technology function will periodically review work areas to determine if UID's and/or passwords have been written down and left in easy-to-find locations. Violations of this policy will be reported to the violator's Department Head and the Town Manager and may result in disciplinary action.

7.5 Responsibilities

Technology Function – Issues UID names and limits access to proper authorized use. Tracks and audits usage for violations of the policy.

Employee's – Maintain confidentiality of UID names and passwords.

Department Heads – Provide disciplinary action for those violating the policy.

8.0 Public Records Requests

8.1 Policy

It is the policy of the Town to direct all computer system public records requests to the Town Clerk's office.

8.2 Purpose/Description

Although much of the information generated by a Town is subject to public records requests, a number of exceptions are provided for in Chapter 119 of the Florida State Statutes. Giving out information that is subject to these exceptions is a serious violation of State Law. All public records requests should therefore be forwarded to the Town Clerk for proper handling. No employee should provide computer information collected or stored by the Town's computers to any individual without first working with the Town Clerk.

8.3 Enforcement

Employees are expected to follow the policy. Violations will be reported to the Department Head and the Town Manager.

8.4 Responsibilities

Employees - Direct public records requests to the Town's Clerk's office.

Town Clerk – Receives and processes requests.

Department Heads – Provide disciplinary action for those violating the policy.

9.0 Instant Messaging/Chat Rooms

9.1 Policy

Installation of Instant Messaging (IM) client software and all related tools (voice chat, file transfer and sharing, etc) is strictly prohibited on Town computers.

9.2 Purpose/Description

Flaws have been found in the client-side software for all major IM programs. These flaws can expose serious vulnerabilities, including buffer overflows that facilitate arbitrary execution of scripts and programs that can upload viruses. None of the major protocols used for chat or instant messaging use encryption, so any sensitive topics discussed using messaging tools are transmitted either. File transfers and sharing capabilities do not offer adequate access controls to prevent misuse and unauthorized access, local file path disclosure, system crashes and denials of service.

9.3 Enforcement

The IT Manager will immediately remove and confiscate any software found in violation of this policy. Incidents will be reported to the employee's Department Head and to the Town Manager.

9.4 Responsibilities

Employees – Shall not utilize or install instant messaging or chat room software.

Technology Function – Audits, removes and reports violations.

Department Heads – Provide disciplinary action for those violating the policy.

10.0 Importing External Data

10.1 Policy

External data that originates from an entity other than a town employee are permitted on any Town owned computer.

Any non-town generated external data, file must be reviewed by the IT Manager **prior** to attempting to import or load it onto a Town owned computer. This includes any file that has been sent by any means, including e-mail. It may be imported by means of any physical portable media (diskette, CD, Zip Disk, etc.). Imported Data to be used in public meeting presentations (PowerPoint) shall be submitted to the IT Manager at least one week prior to the meeting. ***External data submitted to the IT Manager inside the one week time frame will not be allowed on the town network.***

10.2 Purpose/Description

This policy relates to the importing or copying of any file, picture, graphic, logo, or data of any type that does not already reside on the network or in a computer connected to the network. Because the Technology function ensures that Town computers have the latest virus protection software and updates, importing of any Microsoft work file (i.e. Word, Excel, PowerPoint, or Access) is permitted. Other imports with extensions such as EXE, VBS or PIF, etc. may pose a significant threat to the Town's systems and are not to be imported without first being reviewed by the Technology function.

10.3 Enforcement

It is expected that employees will adhere to the policy. Should the Technology function find files that have been imported in abuse of this policy, a report to the violator's Department Head and the Town Manager will be generated for action.

10.4 Responsibilities

End-Users – Work with the Technology function approval and supervision to import non-Microsoft data files.

Technology Function – Works with employees who have a need to import data files that may pose potential hazards.

Department Heads – Provide disciplinary action for those violating the policy.

:

11.0 Data Backup and Recovery

11.1 Policy

Employees will keep critical Town data files on the network file server. Any data not kept on the file server is considered non-critical, non-essential and dispensable. Only network data is backed up for recovery. The Technology function controls all backup and recovery activities.

11.2 Purpose/Description

Information is a critical asset to the Town and must be appropriately protected through an established backup and recovery system. Data can reside either on the main computer systems, the Town's network or the employee's local personal computer (PC). **Only data residing on network servers and drives will be backed up. It is strongly recommended that important data be saved to a network drive and not on the local client computer**.

The Technology function is responsible for backing up the main computer systems and the network file servers at all locations.

Nightly (Monday through Friday), backups are made of the data on all Town servers in the following order…

AP server ?????? PD Server
PD Server ?????? AP Server
Mail Exchange ???? PD Server
IMS ????????? PD Server
Fireserver ?????? Fireserver

Daily, backup tapes from each server are rotated to an off-site storage location.

A complete backup of the servers will be performed once a month and the tapes stored to an off-site location.

The Technology function is also responsible for restoring the systems in the event of a disaster. Should a disaster occur during the day information processed that day may be lost. It will then be the responsibility of the employee to reconstruct that day's work.

11.3 Backup Audit Logs

The Technology function will maintain a log of all backup tapes. The log shall consist of what is on each of the tapes, the date of the backup, and a notation that the tape was verified to have good information, the location and a signature of the individual certifying the backup process. This log will be maintained in a location that is accessible to the Town Manager and shall be audited periodically.

Monthly backup tapes will not be reused for a period of twelve months, so that there are a set of 12 full monthly backup tapes available at any given point in time.

11.4 Enforcement

It is expected that all parties will adhere to the policy. Should the Technology function find critical Town data files resident on an employee's personal computer; the Technology function will work with the employee to put the files on the main server. Continued abuse of this policy will result in a report to the violator's Department Head and the Town Manager.

The Town Manager or his/her representative will periodically and without notice, audit the backup logs to ensure backups are stored, labeled and rotated properly by the Technology function. Disciplinary action will result if backups are not being executed properly.

11.5 Responsibilities

Employees – Are responsible for saving critical files on the network server so they can be backed up.

Technology Function – Ensures that employees use file servers for data; provides for backup of network data and maintains appropriate logs.

Town Manager – Audits backup logs.

Department Heads – Provide disciplinary action for those violating any part of this policy.

12.0 Modems

12.1 Policy

Modems will not be used within the Town network unless **prior** approval from the IT Manager has been given. If a modem is approved, it must be physically disconnected from the system when not in use. Modems must be purchased and installed by the Technology function.

12.2 Purpose/Description

Modems are used to gain telephone dial-up access to an outside entity for the purpose of importing or exporting data (e.g. Aircard). On some occasions, modems are used to gain entry into a system for the purpose of system maintenance, problem detection, or other such functions. Dial-up access modems pose a significant security threat unless properly controlled.

12.3 Enforcement

Any modem found that has not been approved and installed by the Technology function will be disconnected and confiscated. The incident will be reported to the violator's Department Head and the Town Manager and may result in disciplinary action.

12.4 Responsibilities

Employees – Work with the Technology function for proper approval, purchase and installation.

Technology Function – Authorize, purchase, and install modems when a legitimate business need is present. Remove any unauthorized modem and report violations to the user Department Head and the Town Manager.

Department Heads – Provide disciplinary action for those violating the policy.

:

13.0 Architectural Standards – November 30, 2007

13.1 Policy

It is the policy of the Town to standardize a subset of technology in order to ensure continuity of operations, reduce staffing cost and build a reliable computer environment. The following are the current standards for use when purchasing hardware

and software. No computer equipment other than that which has been approved by the IT Manager will be allowed on the Town network (monitors, jump drives, external drives, PDA's, etc). Any unauthorized equipment found in place will be confiscated immediately.

13.2 Server Operating Systems

The Town will operate under a mixed Microsoft Windows 2000, 2003 network operating system for the foreseeable future. The Windows network will be using native mode Active Directory. Any software systems purchased or developed must conform to either the Microsoft Windows 2000 or Windows 2003 platform. Replacement of town servers will occur not later than 5 years after initial purchase.

13.3 Desktop Client Operating Systems

The Town will remain with the Microsoft Windows operating system for its desktop clients. All software purchased or developed must be compatible with Windows XP or newer. The Town will no longer purchase Windows 98 or Windows ME or Windows 2000 Operating systems for any new computing devices. Replacement of client computers will occur not later than 3 years after initial purchase.

13.4 Network Standards

The Town will utilize category 5e, 100 base "T" Ethernet network systems operating at the 100 megabit/sec level for the foreseeable future, with the possibility of moving to gigabit speeds on both the desktop clients and servers in the next couple of years.

The Town will use a top-named manufacturer for routers, hubs and switches for LAN (Local Area Network) and WAN (Wide Area Network) connectivity. The uniformity of this type of equipment will provide stability to the Town's LAN, WAN and Internet accessibility and connectivity.

Bandwidth between remote Town buildings will be at a minimum 1.5 Mbs (up and down) with the preferred being 3 Mbs or higher. It will be the goal of the Town to achieve the highest possible bandwidth budget will allow.

13.5 Specific Technology Architecture Standards:

	Minimum Acceptable	**Future**
Client OS	Windows XP	Windows XP/Vista
Client Office	MS Office 2003	MS Office 2007
Client CPU	Pentium 4, 3ghz	>= Intel core2 duo, 2.2ghz
Client RAM	1GB	>= 2GB
Client HD	80GB	>= 80GB
Client Monitors	17" Flat panel Monitors	17"/19" Flat panels
Client CD	40x	>= 52x
Client UPS	420V – 600V	>= 500V
	Minimum Acceptable	**Future**
Server OS	Windows 2003 Server	Windows 2003 Server/Longhorn
Server CPU	Intel Pentium 4, 3ghz	>= Intel quad core Xeon, 3ghz
Server #CPU	1 - 2	1 - 2
Server RAM	2GB	>= 4GB
Server HD	18GB – Unlimited	>= 146GB X3
Server RAID	RAID1, RAID5	RAID1, RAID5
Server UPS	1400V – 3000V	>= 1400V (dual)

14.0 Posting Public Notices to Ch 199 and Town Web site

14.1 Policy

It is the policy of the Town to standardize the manner in which town staff posts information for public consumption to the town web site and public access TV channel 199.

14.2 Purpose/Description

Town Manager must approve all public notices followed by Assistant Town Manager and Department Head, in that order if Town Manager is unavailable.
In any situation where the official printed publications of the Town of Ponce Inlet differ from the text contained in this system, the official printed documents take precedence. The services, information, and data made available at the Town of Ponce Inlet website are provided "as is" without warranties of any kind. The Town of Ponce Inlet makes no representations or warranties regarding the condition or functionality of this web site, its suitability for use, or that this web service will be uninterrupted or error-free.
The Town of Ponce Inlet does not accept requests for placing personal, political or commercial advertisements on any part of the town's website.
Data on this system is public information and is generally available to copy or distribute (Ok to post anything that is public records minus any sensitive information such as SS#, police records, etc). Information and/or images which may not be copied without permission includes copyrighted materials, such as artwork contained on the pages and the Town of Ponce Inlet seal.
Any Town sanctioned event may be posted onto the Town News or Community Events sections of the website and Chanel 199 pending the approval of the Town Manager.
Any Public Notice (ie. road maintenance, waste collection, etc) pertaining to the citizens of Ponce Inlet may be posted on the Town News section of the website and Channel 199.

In the event that an item pertaining to the immediate health and welfare of the public needs publication to channel 199 and/or the web site, the above procedure may be waived at the direction of the Police Chief or Fire Chief. The Town Manager (or her designee) must be notified as soon as possible after the posting occurs.

.

14.3 Enforcement

It is expected that employees will adhere to the policy. Should any item be published to the web site or channel 199 without following the above procedure, a report to the violator's Department Head and the Town Manager will be generated for action.

15.0 Surplus Technology Equipment Management

15.1 Policy

All town owned technology equipment shall be surplused in the most economically and environmentally friendly manner possible. This includes all client computers and servers replaced by new equipment.

15.2 Purpose/Description

All technology equipment that is no longer of institutional value, damaged, or obsolete shall be surplused in accordance with established Town policy. All surplused computers and servers shall be removed from the TPI domain and reset as an individual workgroup computer/server. Computers declared as surplus and being purchased by employees will have all town related material deleted from the hard drives. Surplus computers and servers being sent to auction will have the hard drives removed, magnetized and physically distorted. Only computers and servers without hard drives will be sent to auction.
Other obsolete technology items will be surplused or discarded per established Town policy and procedures.
The IT Manager will compile a list of all equipment meeting the surplus designation for each department and provide the list to the appropriate asset manager. The list will include make, model, and serial number of the computer/server. Surplus computers to be purchased by employees will include all recovery/driver disks and operating system (if available).

Surplus computer equipment sold to employees or at auction will be sold "as is" with no warranty, guarantee, or technology support from the Town.

15.3 Enforcement

It is expected that employees will adhere to the policy. Any questions as to financial or functional value of a piece of technology equipment shall be directed to the IT Manager for review.