HAMPTON VA

No. IT– 038	Policy Name: Public Computing Policy
Effective Date: 7-1-2011 Last Revised Date: 6-25-2014	Citywide Policy X IT Policy _ IT Procedure _
Approved By: IT Director	

City Provided Public Computing Services

I. The purpose of this policy is to provide guidance to departments to ensure the safety, security and reliability of public computing services in the City of Hampton.

II. Overview: Currently the City has two categories of service delivery for providing public computing resources. The City's Information Technology department does not provide public computing services due to resource constraints. Therefore, this policy documents department options and responsibilities for providing these services to the public. Generally, there are two models utilized by City departments providing public computing services.

1. **City Provided:** City Departments providing and managing computing services directly to citizens to provide their department's services more effectively to citizens. In these cases the devices are owned and managed by the City and these departments follow the City's IT policies and procedures found in the current Tech Manual. The City Library is an example of this model where Library personnel manage all public computing services provided in their facilities.
2. **Partnership Provided:** In the partnership provided model, city departments provide computing services to citizens at a City location through a volunteer, non-profit or other private organization. In these cases the outside organizations provide support for computers, software, training, upgrades and other desktop features and functions. Examples of this model include the Parks and Recreation Department computing resources in the New Town Learning Center and YH Thomas.

III. Equipment & Software

Departments procuring or receiving donations of equipment for public computing purposes will utilize standard City procurement processes.

Donated equipment will have all previous data wiped off the system(s) prior to deployment to ensure the security and integrity of the system prior to placement in service.

All software procured, downloaded, received and installed shall be legally obtained and licensed. On occasion City departments may wish to donate used City devices for public computing purposes. Any City assets transferred for the purpose of public computing will have all data permanently removed from the device prior to the asset being placed into public computing service. This may require removal or destruction of the hard drive and/or the loss of software licenses attached to the transferred device. Taking these steps ensures that no sensitive City data is available to unauthorized users. See Data Disposal Policy IT-030

IV. Network Resources and Support

Departments providing public computing services will utilize Internet service providers and contracts outside of the City's standard, internal network services. The IT department can assist with finding appropriate Internet Service Providers for public computing needs. Departments or their public computing partners will be responsible for the following tasks:

A. Ordering, provisioning and payment for services and equipment to providers
B. Connecting and monitoring computing resources on the network
C. Securing network resources
D. Managing network capacity and usage
E. Troubleshooting and resolving network issues
F. Coordinating with the City IT Department on network issues and providing the City IT department with points of contact for addressing any emergency issues.

V. Desktop & End User Support

1. Departments will provide a point of contact for to the IT department for each public computing facility for coordination purposes.
2. Citizens utilizing public computing will not contact the City's IT department directly with problems or issues. These will be reported and coordinated through the department's public computing support staff or service partners.

VI. Technology Refresh

1. Departments are responsible for ensuring the software and hardware on public computing devices is refreshed and upgraded based on the requirements of the users. Departments or their partners will fund the purchase or upgrades of hardware and software as appropriate. For instance, if classes are taught on a specific software package, departments will be responsible for ensuring that the software has been obtained legally and is installed correctly for use by the students and within a reasonable timeframe to test the new services.
2. The IT Department may assist with refresh plans and can suggest resources to assist with refresh and upgrade implementations at the Department's request. City IT Department staff will generally not be available to implement technology refresh and upgrades for public computing environments.

VII. Partnership Requirements

1. Departments utilizing the partnership model for public computing support shall develop a memorandum of agreement or contract for services. The memorandum of agreement should be in place prior to services being performed by the partner. The agreement should address the following items at a minimum.
   A. Partners shall certify that and warrant that any software provided by or procured by the partner has been legally obtained and licensed. This includes software that has been downloaded, purchases, received and installed in any form or fashion for use by the public computing environment. In addition, the partners shall agree to hold the City of Hampton, City departments and employees of the City harmless for any liability if they (the partner) fails to do so.
   B. Partners are responsible for following all City of Hampton security policies and procedures at a minimum. Additional or more stringent policies may be added by the partner. All additions or changes to security policies and procedures shall be reviewed and approved by the IT Governance Board and the IT Director prior to implementation.
   C. The scope of work and roles and responsibilities of the partner and the City department overseeing the public computing services.
   D. Identify any fees or costs associated with supporting the public computing center and who is responsible for payment and the process for payment.
   E. Hours of support and processes for reporting problems and requests for support
   F. Location of support services and any requirements for physical access and physical security.
   G. Inventory of equipment supported and identify who will be responsible for asset management and inventory control for public computing devices.

VIII. Security

1. Public computing centers will follow the City's information security policies and procedures found in the most recent Tech Manual.
2. Departments providing public computing services have the option of following the City's information security policies and procedures or developing their own for public computing centers.
    A. Those that develop their own will submit their security policies and procedures to the IT department, the IT Governance Board and the City Attorney's Office for review and approval.
    B. Enforcement and training on the policy will be the responsibility of the department. Departments may ask the IT Department to assist with enforcement and training issues. The IT Department will make every effort to assist using current staff but may need to bring in outside resources as issues needed.
3. All public computing services should have the following minimum standards met.

    A. Processes to ensure citizen and employee personal data is not saved or stored on computers or network devices. This includes but is not limited to social security numbers, passwords, bank account numbers, credit card numbers, employee numbers, log ons, or other data that could lead to identify theft or other illegal activities.
    B. Processes to ensure illegal activity is not taking place utilizing public computing resources
    C. Processes to ensure viruses, worms, and other malicious code is not developed, stored, deployed or passed to others from the computing environment. Anti virus software will be installed on all public computing devices.
    D. Processes to ensure public computers do not become devices to spread SPAM or other services which may lead the City to become a nuisance to other users within or outside of the City.

4. Any security breaches in a public computing environment identified in 3. above will require the immediate notification to the Department Head. In addition the department will notify the IT department though an e-mail sent to IThelp@hampton.gov or by calling 311.

5.Public Computing to Minors – Departments that provide public computing services to minors will develop, maintain, implement and enforce a computer security program based on the Virginia Department of Education's resources on Internet Safety. The policy and procedures will be approved by the public computing department, the IT Governance Board and the City Attorney's Office. http://www.doe.virginia.gov/support/safety_crisis_management/internet_safety/index.shtml

Note: The City's Library system utilizes an automated product called Envisionware to provide this and other types of protection. Other solutions are available to manage public computing environments securely. Departments are encouraged to research and implement public computing management tools.