RESOLUTION 287

IT Policy Training

This page intentionally left blank.

PUTNAM COUNTY SECURITY AND IT USE POLICY

Information and information systems are key assets of Putnam County ("the County"). They are essential to the conduct of County business and are a part of most employees' daily work. The County provides systems, including the computers, networks, technology applications and the information housed therein to permit employees to perform their duties more effectively.

This policy sets forth a basic set of standards for use and protection of computer and information assets. It includes but is not limited to computer workstations, laptop computers, electronic mail ("e-mail"), databases, networks and connection(s) - both wired and wireless - to the intranet, Internet and any other information technology services available both now and in the future.

This policy covers all employees of Putnam County. It also covers any other individuals, including consultants, interns, temporaries and vendors, who have access to County technology facilities, computers or networks.

Inappropriate use of equipment and services exposes the County to risks including virus attacks, system compromise, interruption of services and legal issues.

Effective security is a team effort involving the participation and support of every County employee and affiliate who deals with data and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

I. Prohibited Uses of County IT Equipment, Domains and Emails

Under no circumstances may any voicemail, email, or other electronic communication or posting originating from the County, created on County equipment, created by employees, intentionally received at the County, or related to or referencing the County, your relationship with the County or any other employee be in violation of the letter or spirit of the County's policies concerning equal opportunity, discrimination, harassment or be of a nature that may create a hostile or inappropriate work environment.

The County owns various domains, including but not limited to *putnamcountyny.gov* and *putnamcountyny.com,* including the email address provided to you by the County. For a current list of County owned domains, please contact the office of IT/GIS. All employees should remember that any email sent from a County owned domain is identifiable and attributable to the County. As such, every email sent from said domains must comply with this IT policy without exception.

The following would constitute improper use of your County owned domain as a return email address: including but not limited to: placing an email address on a website to allow visitors to contact you for further information for reasons unrelated to your job duties or without authorization from your department head; using an email address to create a personal account on a social media network such as Facebook, Twitter, etc.; using a County email address to place a

"Personal" order unrelated to county business online. When a County owned domain is used for any reason, it must conform to this policy.

The County system (including County-owned domains/emails) shall not be used for any illegal activities or activities the County deems to be improper, including, but not limited to: activities unrelated to the County's mission; misrepresenting, obscuring, suppressing or replacing any identity on an electronic communication; using County IT equipment to engage in any business activity outside of the County; for any purpose contrary to the County's policy or business interests; gambling; any unauthorized attempt to compromise computer or communication security or otherwise interfere with or disrupt network users, services or equipment; any use that violates federal, state or local law or regulation; or using the County network to gain unauthorized access to any computer system. Employees who encounter such material on County equipment or elsewhere should immediately report it to their supervisor, the Personnel Department or the Director of IT/GIS.

All emails sent from the County owned domains shall, at a minimum: be courteous and follow accepted standards of etiquette; be professional, ethical, and of a lawful manner; protect others' privacy and confidentiality; comply with County department and unit policies, procedures and standards; be complete, accurate and truly representative of the County's position.

Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by a Department Head and by the Director of IT/GIS or his/her designee via written or email request, employees are prohibited from engaging in, or attempting to engage in the following: monitoring or intercepting the files or electronic communications of other employees or third parties; hacking or obtaining access to systems or accounts they are not authorized to use; using other people's log-ins or passwords; and breaching, testing, or monitoring computer or network security measures. Furthermore, no email or other electronic communications can be sent that attempt to hide the identity of the sender or represents the sender as someone else.

It is best to be fair and respectful to fellow employees, community members, and those who work on behalf of the County or the County's legitimate business interests. Employees shall not post complaints or criticism using statements, photographs, videos, or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating or that might constitute a violation of the County's Workplace Violence Policy, discrimination or harassment on the basis of race, sex, disability, religion or any other status protected by law or any County Policy.

II. No Expectation of Privacy Concerning use of County IT Equipment, Domains and Emails

Putnam County maintains the right to access and examine County computer systems and networks and all information that is stored or transmitted through these systems and networks, including all e-mail and website visits. All electronic communications are considered County records. As County records, electronic communications are subject to disclosure to law enforcement or government officials or to other third parties through FOIL (Freedom of Information Law) request or other process. Employees must ensure that information contained in electronic

communications is accurate, appropriate and lawful.

While Putnam County does not intend to regularly review employees' e-mail records, employees have no right or expectation of privacy in e-mail. Since the County is responsible for the servicing and protecting of its electronic communications networks and administering this policy, it is occasionally necessary to intercept or disclose electronic communication.

Communications on these Systems are not private. Users should be aware that the data they create on the System remains the property of the County, and usually can be recovered even though deleted by the user. Despite security precautions, there is no absolutely fail-safe way to prevent an unauthorized user from accessing stored files. The confidentiality of any information stored or transmitted on the System cannot be guaranteed. Furthermore, information that is stored on the System or sent via e-mail may be subject to disclosure pursuant to the New York State Freedom of Information Law.

III. Personal Use of County Equipment and Systems

The County permits incidental personal use of its electronic communication tools with the express understanding that it reserves the right to restrict access to sites, and/or to review all use of, and to monitor, observe and inspect all communications and material created by, stored, in transit, or transmitted on, electronic communication tools, and with the express understanding that such use may not interfere with or preempt the employee from completing his/her work as necessary. Employees are not permitted to engage in such incidental use where such use consumes a significant amount of resources that could otherwise be used for business purposes, interferes with an employee's productivity and preempts or interferes with any business activity or is contrary to any County policies.

IV. Social Media

Although social media technology is constantly changing, this policy was developed to cover Putnam County employee and County Network user participation in all forms of communicating or posting information or content via the Internet, including, but not limited to, social networking sites (for example, FaceBook, LinkedIn), blogs, Twitter accounts, video- or photo -sharing sites, websites, chat rooms, and other forms of online dialogue.

All County employees and Network users must at a minimum adhere to the following rules when using social media technologies on County IT resources and/or in their capacities as a County employee:

- Use of social media may not interfere with any employee's productivity or detract resources from performing assigned business related duties.
- Social media behavior may in no way harm or tarnish the image, reputation and/or good will of the County and/or any of its employees.

- Employees are prohibited from making any discriminatory, disparaging, defamatory or harassing comments when using social media or otherwise engaging in any conduct prohibited by the County's policies concerning equal opportunity, discrimination, harassment.
- Are responsible for all of their online activities that are conducted with a County e-mail address, can be traced to a County domain and/or uses County resources.
- Must not discuss or post confidential, proprietary or otherwise restricted information.
- When speaking on behalf of the County in an official capacity, users must be transparent when participating in any online community. They should disclose their identity and affiliation with the County government entity.
- Communicate in a professional manner.
- Abide by copyright and other applicable laws. Participation online results in a user's comments being permanently available and open to being republished in other media. Users should be aware that libel, defamation, copyright and data protection laws apply.
- When communicating on behalf of the County, County employees must obtain necessary authorizations by the County Executive and/or the appropriate Department Head and/or designee.
- Must obtain permission before publishing photographs, videos or quotes of others.
- When not representing the County government entity, County employees who publish personal or professional opinions must not invoke their County government title. In such cases, users must use a disclaimer such as the following where technically feasible: "The postings on this site are my own and do not represent the position, strategy or opinion of Putnam County Government (or other County department/entity).

V. Prohibited Connections to County Network

For the purpose of this policy, personal electronic devices include but are not limited to personally owned cell phones, tablets, printers, laptops and computers. Peripheral equipment includes but is not limited to thumb drives, USB sticks and/or mass storage devices, speakers, mice and keyboards. County owned networks include but are not limited to the County's hard wired network and the County's Wireless Access Points that are secured with a password. The County does maintain "open" public Wireless Access Points that do not require a password to connect. While these points are open for public use and employees may connect to them without permission, all uses of these points are required to conform to the provisions of this policy.

Under no circumstances are employees permitted to connect personal electronic devices and/or peripheral equipment to County owned network through wireless or direct connection without express permission from the Director of IT/GIS. Failure to obtain permission will be considered a security breach and may result in not only employee disciplinary action but possible criminal charges. The County's network must be protected at all times and the connection of unknown and unmonitored equipment provides an extreme risk that will result in serious action.

VI. Security

Each individual must be positively identified prior to being able to use any County computer or communications system resource. Positive identification for internal County networks involves a User-ID and a password, both of which are unique to an individual and will be supplied by IT upon employment. Each person must log off from all User-ID accounts before leaving at the end of their workday. Each person is responsible for all activity that occurs on his or her User-ID. User-ID's will be revoked if the employee is terminated. Employees cannot share their passwords with other employees, and supervisors cannot ask employees for their password.

To prevent computer viruses from being transmitted through the County's computer system, installation of software may only be performed by the County IT Department. Only software registered through the County and authorized by the County IT Department may be downloaded. Employees should contact the Director of IT if they have any questions. In addition, Employees must use extreme caution when opening e-mail attachments and/or clicking on links received from unknown senders, which may contain virus, e-mail bombs or Trojan horse code. Should an employee receive a suspicious e-mail, the e-mail should be deleted immediately and should not be forwarded. The employee should then alert IT of the nature of the e-mail received. If an employee clicks on a suspicious link in an e-mail or on the internet, the employee should immediately stop using the computer, disconnect the network cord from the wall (or the power cord if the network cord cannot be identified) and contact IT.

VII. Encryption & Removal of County Owned Data

Employees can use encryption software supplied to them by the IT Department for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a County computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files. It is mandatory that any data removed from the County premises be encrypted, without exception. This is particularly true if the data is on a thumb drive, media CD, etc. Encryption ensures that in the event the object is lost or stolen, the receiver would be unable to read or access the data without specific passwords or codes.

Data belonging to the County shall not be removed from County premises without express permission from the owner of the data, the department head of the owner of the data, or the Director of IT/ GIS. This includes, but is not limited to the use of: thumb drives; cloud services; direct data transfer to personal computer or other devices; CDs, DVDs, or other media; or any device or service that allows data to be removed from its original storage location.

VIII. Violations

All Employees are responsible for complying with this policy and reporting any known or suspected violation of this policy to their immediate supervisor or the Department of Information/GIS. The County prohibits taking any negative or improper action against any other employee who reports a violation of this policy. Employees who violate this policy will be subject to appropriate

disciplinary and/or legal action, up to and including termination.