

Communication Media Policy: *

The Borough's Communication Media are the property of the Borough and, as such, are to be used for legitimate business purposes only. For purposes of this Communication Media Policy, "Communication Media" includes all electronic media forms provided by the (local unit type), such as cell phones, smart phones, computers, electronic tablets, access to the internet, voicemail, email, and fax.

All data stored on and/or transmitted through Communication Media is the property of the (local unit type). For purposes of this policy, "Data" includes "electronically-stored files, programs, tables, databases, audio and video objects, spreadsheets, reports and printed or microfiche materials which serve a (local unit type) business purpose, regardless of who creates, processes or maintains the data, or whether the data is processed manually or through any of the (local unit type's) mainframe, midrange or workstations; servers, routers, gateways, bridges, hubs, switches and other hardware components of the (local unit type's) local or wide-area networks."

The Borough respects the individual privacy of its employees. However, employee communications transmitted by the Borough's Communication Media are not private to the individual. All Communication Media and all communications and stored information transmitted, received, or contained in or through such media may be monitored by the Borough. The Borough reserves the absolute right to access, review, audit and disclose all matters entered into, sent over, placed in storage in the Borough of South Toms Rivers Communication Media. By using the Borough's equipment and/or Communication Media, employees consent to have such use monitored at any time, with or without notice, by Borough personnel. The existence of passwords does not restrict or eliminate the Borough's ability or right to access electronic communications. However, the Borough cannot require the employee to provide its password to his/her personal account.

All email, voicemail and Internet messages (including any technology-based messaging) are official documents subject to the provisions of the Open Public Records Act (NJSA 47:1A-1). Employees of the Borough are required to use the assigned municipal email account for ALL Borough business and correspondence. The use of private email accounts for ANY Borough business or during business hours is strictly prohibited.

Employees can only use the Borough's Communication Media for legitimate business purposes. Employees may not use Borough's Communication Media in any way that is defamatory, obscene, or harassing or in violation of any Borough rules or policy. Examples of forbidden transmissions or downloads include sexually-explicit messages; unwelcome propositions; ethnic or racial slurs; or any other message that can be construed to be harassment or disparaging to others based on their actual or perceived age, race, religion, sex, sexual orientation, gender identity or expression, genetic information, disability, national origin, ethnicity, citizenship, marital status or any other legally recognized protected basis under federal, state or local laws, regulations or ordinances.

All employees, who have been granted access to electronically-stored data, must use a logon ID assigned by the Borough. Certain data, or applications that process data, may require additional security measures as determined by the Borough. Employees must not share their passwords; and each employee is responsible for all activity that occurs in connection with their passwords.

All employees may access only data for which the Borough has given permission. All employees must take appropriate actions to ensure that Borough data is protected from unauthorized access, use or distribution consistent with these policies. Employees may not access or retrieve any information technology resource and store information other than where authorized.

Employees must not disable anti-virus and other implemented security software for any reason, in order to minimize the risk of introducing computer viruses into the Borough's computing environment.

Employees may not install *or Modify* ANY hardware device, software application, program code, either active or passive, or a portion thereof, without the express written permission from the Borough. Employees may not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the Borough, or licensed to the Borough. Employees shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.

The Borough encourages employees to share information with co-workers and with those outside the Borough for the purpose of gathering information, generating new ideas and learning from the work of others to the extent such sharing is permitted by the Borough. Social media provide inexpensive, informal and timely ways to participate in an exchange of ideas and information. However, information posted on a website is available to the public; therefore, employees must adhere to the following guidelines for their participation in social media. Employees may engage in social media activity during work time through the use of the Borough's Communication Media, provided that it is directly related to their work and it is in compliance with this policy.

Employees must not reveal or publicize confidential Borough information. Confidential proprietary or sensitive information may be disseminated only to individuals with a need and a right to know, and where there is sufficient assurance that appropriate security of such information will be maintained. Such information includes, but is not limited to the transmittal of personnel information such as medical records or related information. In law enforcement operations, confidential, proprietary or sensitive information also includes criminal history information, confidential informant identification, and intelligence and tactical operations files.

Employees are prohibited from releasing or disclosing any photographs, pictures, digital images of any crime scenes, traffic crashes, arrestees, detainees, people or job related incident or occurrence taken with the Borough's Communication Media to any person, entity, business or media or Internet outlet whether on or off duty without the express written permission of the Clerk/Administrator or police chief. Except in "emergency situations, "Employees are prohibited from taking digital images or photographs with media equipment not owned by the Borough. For purposes of this section, an "emergency situation" involves a sudden and unforeseen combination of circumstances or the resulting state that calls for immediate action, assistance or relief, and may include accidents, crimes and flights from accidents or crimes and the employee does not have access to the Borough's Communication Media. If such situation occurs, employee agrees that any images belong to the Borough and agree to release the image to the Borough and ensure its permanent deletion from media device upon direction from the Borough.

No media advertisement, electronic bulletin board posting, or any other posting accessible via the Internet about the Borough or on behalf of the Borough, whether through the use of the Borough's Communication Media or otherwise, may be issued unless it has first been approved by the Clerk/Administrator. Under no circumstances may information of a confidential, sensitive or otherwise proprietary nature be placed or posted on the Internet or otherwise disclosed to anyone outside the Borough.

Because authorized postings placed on the Internet through use of the Borough's Communication Media will display on the Borough's return address, any information posted on the Internet must reflect and adhere to all of the Borough's standards and policies.

All users are personally accountable for messages that they originate or forward using the Borough's Communication Media. Misrepresenting, obscuring, suppressing, or replacing a user's identity on any Communication Media is prohibited. "Spoofing" (constructing electronic communications so that it appears to be from someone else) is prohibited.

Employees must respect the laws regarding copyrights, trademarks, rights of public Borough and other third-party rights. Any use of the Borough's name, logos, service marks or trademarks outside the course of the employee's employment, without the express consent of the Borough, is strictly prohibited. To minimize the risk of a copyright violation, employees should provide references to the source(s) of information used and cite copyrighted works identified in online communications.

To the extent that employees use social media outside of their employment and in so doing employees identify themselves as Borough employees, or if they discuss matters related to the Borough on a social media site, employees must add a disclaimer on the front page, stating that it does not express the views of the Borough, and the employee is expressing only their personal views. For example: "The views expressed on this website/web log are mine alone and do not necessarily reflect the views of my employer." Place the disclaimer in a prominent position and repeat it for each posting that is expressing an opinion related to the Borough or the Borough's business. Employees must keep in mind that, if they post information on a social media site that is in violation of Borough policy and/or federal, state or local laws, the disclaimer will not shield them from disciplinary action.

Nothing in these policies is designed to interfere with, restrain or prevent employee communications regarding wages, hours or other terms and conditions of employment. Borough employees have the right to engage in or refrain from such activities.