

From: Chris Wood
Sent: Tuesday, July 23, 2019 9:32 AM
To: Karen Gallagher
Subject: FW: OPRA request - Facebook policies and procedures

RECEIVED

JUL 23 2019

CITY CLERK'S OFFICE

-----Original Message-----

From: Anonymous [mailto:opra+request-6410-6747a457@requests.opramachine.com]
Sent: Monday, July 22, 2019 4:13 PM
To: Chris Wood
Subject: OPRA request - Facebook policies and procedures

Dear Wildwood City,

This is a request for public records made under OPRA and the common law right of access. I am not required to fill out an official form. Please acknowledge receipt of this message.

Records requested:

1. A copy of policies and/or procedures regulating the Wildwood public facebook page, any and all Wildwood, policies regarding the maintenance and/or content retention of township maintained social media forums.
2. List(s) of names of people who are/were hidden, blocked, banned from the Wildwood,public facebook page.
3. List(s) of any deleted, hidden, blocked, banned comments that were on the Wildwood Office's public facebook page for the time period of 1-1-2018 to 7-1-2019.
4. List(s) of the authors' names of any deleted, hidden, blocked, banned comments that were on the Wildwood, public facebook page for the time period of 1-1-2018 to 7-1-2019.
5. Copies of all messages and author's names sent via the Wildwood, facebook messenger and responses for the time period of 1-1-2018 to 7-1-2019.
6. Name and rank and/or position title of the Wildwood, employee(s) responsible for maintaining any and all Wildwood, social media forums.
7. Any emails sent to/from the employee(s) in question regarding the deleting/removing of content, or the limiting of access to content on any and all social media forums for the time period of 1-1-2018 to 7-1-2019.

Yours faithfully,

Anonymous

Please use deliver records electronically via email to the below UNIQUE address for all replies to this request:
opra+request-6410-6747a457@requests.opramachine.com

Is cwood@wildwoodnj.org the wrong address for OPRA requests to Wildwood City? If so, please contact us using this form:
https://opramachine.com/change_request/new?body=wildwood_city

Disclaimer: This message and any reply that you make will be published on the internet. Our privacy and copyright policies:
<https://opramachine.com/help/officers>

View this OPRA request & responses online:
https://opramachine.com/request/facebook_policies_and_procedures_57

Please note that in some cases publication of requests and responses will be delayed.

If you find this service useful as an OPRA custodian, please ask your web manager to link to us from your organisation's website.

Communication Media Policy/Social Media Policy:

The City Communication Media are the property of the City 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 City, such as cell phones, smart phones, computers, electronic tablets, access to the internet, voicemail, email, and fax. Employees are restricted from accessing or using the company's Communication Media for personal purposes during company time on company equipment without prior authorization from the Administration to do so.

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

The city respects the individual privacy of its employees. However, employee communications transmitted by the city'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 City. The City reserves the absolute right to access, review, audit and disclose all matters entered into, sent over, placed in storage in the City's Communication Media.** By using the city's equipment and/or Communication Media, employees consent to have such use monitored at any time, with or without notice, by city's personnel. The existence of passwords does not restrict or eliminate the city's ability or right to access electronic communications. However, pursuant to New Jersey Law the city's cannot require the employee to provide the password(s) to his/her personal account(s).

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 city are required to use the assigned municipal email account for ALL city business and correspondence. The use of private email accounts for ANY city business or during business hours is strictly prohibited. Employees are hereby advised that if they conduct work-related business on their personal emails, cell phones, or other personal Communication Media, it is also subject to the provisions of the Open Public Records Act. However, nothing in this social media policy prevents employees from using his/her own personal Communication Media during the employee's non-working hours to engage or participate in protected concerted activities pursuant to the National Labor Relations Act. Protected concerted activities include when an employee addresses group concerns with the employer; forms, joins or helps a labor organization; initiates, induces or prepares for group action; or speaks on behalf of or represents other employees. Nevertheless, employees are encouraged to resolve workplace grievances internally by discussing issues with their supervisor and/or the Administration, and are asked to refrain from posting comments or materials on

Communication Media that can be viewed as malicious, obscene, threatening, intimidating, or that could create a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law if the employee chooses to address their grievances using Communication Media.

Employees can only use the city's Communication Media for legitimate business purposes. Employees may not use city's Communication Media in any way that is defamatory, obscene, or harassing or in violation of any city 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. Further, discriminatory remarks, harassment, bullying, threats of violence and similar behavior that is not tolerated in the workplace are also not acceptable through Communication Media, whether same is performed on the city equipment or on the employee's own personal Communication Media.

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

Information security is necessary to protect the city's information (data and software) from accidental or intentional unauthorized disclosure, modification, or loss. Information security is managed under guidelines dealing with identification, authentication, authorization, production environment, and ability to audit. All employees should be familiar with such security measures adopted by the city.

All employees may access only data for which the city has given permission. All employees must take appropriate actions to ensure that city 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. All (local unit type) data must be stored centrally as required by city. This provides greater security, and ensures backup of all city data is performed.

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 city's computing environment.

Employees may not *Modify or Remove* ANY hardware device, software application, program code, either active or passive, or a portion thereof, without the express written permission from the city. Employees may not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the city, or licensed to the city. 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. . Workstation settings and configurations and network settings must not be modified by unauthorized employees. Internet security settings (where applicable) must not be changed. The foregoing includes but is not limited to the systems Network ID (or Computer Name), IP Address, Gateway and DNS addresses etc.

Social Media and its uses in government and daily life are expanding each year 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. Only those Employees directly authorized by the Administration may engage in social media activity during work time through the use of the city's Communication Media, as it directly relates to their work and it is in compliance with this policy.

Employees must not reveal or publicize confidential city 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.

No City employee shall post internal working documents to social media sites. This includes, but is not limited to, screenshots of computer stations, pictures of monitors and/or actual documents themselves without the prior approval of the Commissioners. In addition 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 city'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 Commissioners. Except in "emergency situations, "Employees are prohibited from taking digital images or photographs with media equipment not owned by the city. 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 city's Communication Media. If such situation occurs, employee agrees that any images belong to the city and agree to release the image to the city and ensure its permanent deletion from media device upon direction from the city.

No media advertisement, electronic bulletin board posting, or any other communication accessible via the Internet about the city or on behalf of the city, through the use of the city's Communication Media may be issued unless it has first been approved by the city's Administration. Specifically, employees are forbidden from using the city's Communication Media to impersonate the employer; to make statements on behalf of the employer without authorization; and/or to make statements that can be construed as establishing what the employer's official position or policy is on any particular issue. In addition, employees are prohibited from placing or posting on the Internet through the employer's Communication

Media or the employee's own personal media, either during working or non-working hours, any employer-related confidential, sensitive or other employer information of a proprietary nature, including but not limited to employer records or documents, trade secrets, internal reports, tips based on inside information that may be considered insider trading, screenshots of computer stations, pictures of monitors and/or actual documents of the employer, any photographs, pictures, digital images of any crime scenes, traffic crashes, arrestees, detainees, people or job-related incidents or occurrences.

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

All users are personally accountable for messages that they originate or forward using the city'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 without a legitimate authorized purpose and authorized by the Commissioners is prohibited

Employees must respect the laws regarding copyrights, trademarks, rights of public city and other third-party rights. Any use of the city's name, logos, service marks or trademarks outside the course of the employee's employment, without the express consent of the city, 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.

If employees choose to identify themselves as a City of Wildwood employee on their personal social media accounts and even those that do not should be aware that he or she may be viewed as acting on behalf of the City, as such no employee shall knowingly represent themselves as a spokesperson of the City, post any comment, text, photo, audio, video or other multimedia file that negatively reflects upon the City expresses views that are detrimental to the City's mission or undermine the public trust or is insulting or offensive to other individuals or to the public in regard to religion, sex, race or national origin. City of Wildwood employees are encouraged to exercise extreme caution posting photographs of themselves in uniform or in situations where they can be readily identified as Township employees.

To the extent that employees use social media outside their employment while engaging in protected concerted activities as defined above, employees will not be subject to discipline or retaliation for expressing views, opinions, and/or facts surrounding the city's employment policies. For all other communications by employees on personal social media sites in which matters related to the city are discussed, employees must add a disclaimer on the front page stating that the posting does not express the views of the city, and that the employees are expressing their own 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.” The disclaimer must be placed in a prominent position and repeated for each posting that is expressing an opinion related to the city or the city’s business, with the exception of postings and social media communications by employees engaging in protected concerted activities. Employees are advised that if they post information on social media that is in violation of either the terms and conditions of the within social media policy, or in violation of federal, state, or local laws, the disclaimer will not shield them from disciplinary action. However, no retaliation or discipline will result if and when employees are engaging in protected concerted activity, and/or choose to report inappropriate social media activities to the City Administration.

Nothing in these policies is designed to interfere with, restrain, or prevent social media communications by employees engaging in protected concerted activities regarding wages, hours, or other terms and conditions of employment pursuant to the National Labor Relations Act. All City employees have the right to engage in or refrain from such activities.