
Electronic Communication

204.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper use and application of the Department's electronic communication systems by employees of this department. Electronic communication is a tool available to employees to enhance efficiency in the performance of job duties and is to be used in accordance with generally accepted business practices and current law (e.g., California Public Records Act). Messages transmitted over the Department's electronic communication systems must only be those that involve official business activities or contain information essential to employees for the accomplishment of business-related tasks and/or communication directly related to the business, administrations or practices of the Department.

204.2 EMAIL RIGHT OF PRIVACY

All email messages, including any attachments, that are transmitted over department networks are considered department records and therefore are department property. The Department reserves the right to access, audit or disclose, for any lawful reason, any message including any attachment that is transmitted over its email system or that is stored on any department system.

The email system is not a confidential system since all communications transmitted on, to or from the system are the property of the Department. Therefore, the email system is not appropriate for confidential communications. If a communication must be private, an alternative method to communicate the message should be used instead of email. Employees using the Department's email system shall have no expectation of privacy concerning communications utilizing the system.

Employees should not use personal accounts to exchange email or other information that is related to the official business of the Department.

204.3 CHECKING EMAIL AND THE CRIME FORUM

Employees shall check their email and Crime Forum accounts for new messages or posts at least two times each duty shift.

- (a) It is recommended that the accounts be checked close to the beginning and end of each shift in order to maximize the employee's exposure to new email messages and crime information.

When requested by the sender of a message, or as otherwise necessary or appropriate, employees shall respond to received email in a timely fashion.

Mis-addressed email should be sent back to the original sender with an advisement that the message was mis-addressed.

Employees may forward or re-distribute copies of email messages only when doing so fulfills a legitimate work-related purpose.

Berkeley Police Department

Law Enforcement Services Manual

Electronic Communication

204.4 PROHIBITED USE OF EMAIL

Sending email messages which are derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing or in any other way inappropriate, is prohibited and may result in discipline.

Email messages addressed to the entire department should only be used for official business related items that are of particular interest to all users. Personal advertisements are not acceptable. Email messages addressed to the entire city must be approved by the Chief of Police or City Manager.

204.5 SECURITY

It is a violation of this policy to transmit a message under another employee's name. Employees are strongly encouraged to log off the network when their computer is unattended.

Employees should protect the security of their network, email and Crime Forum accounts by regularly changing their passwords.

Employees shall not share their passwords with any other individual.

The unauthorized use, or attempted use, of another employee's password, computer files or email without that person's expressed consent is prohibited.

An employee who observes another person use a departmental communication system inappropriately shall immediately notify their supervisor, or if unavailable, the next person in their chain of command.

204.6 EMAIL RECORD MANAGEMENT

Email may, depending upon the individual content, be considered a public record under the California Public Records Act and must be managed in accordance with the established records retention schedule and in compliance with state law.