

CATEGORY	DATE ADOPTED	LAST REVIEW	NEXT REVIEW
3	03/31/2015	12/05/2023	12/05/2026

BUENA PARK POLICE DEPARTMENT GENERAL ORDERS

POLICY 342 DEPARTMENT TECHNOLOGY / E-MAIL USE

342.1 PURPOSE AND SCOPE

This policy describes the use of Buena Park Police Department computers, software, and systems. It establishes guidelines for the proper use and application of electronic mail (email) by employees of this Department.

Employees who choose to access their email accounts from computers outside the Department do so on a voluntary basis and will not be compensated.

342.1.1 ACCREDITATION STANDARDS

This policy pertains to the following CALEA Standards: 11.4.4, 12.1.4, 26.1.3, 41.3.7.

342.1.2 DEFINITIONS

Computer System: All computers (on-site and portable), hardware, software, and resources owned, leased, rented, or licensed by the Department that are provided for official use by Department employees. This shall include all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department or Department funding.

Hardware: Includes, but is not limited to, computers, computer terminals, network equipment, and any other tangible computer device generally understood to comprise hardware.

Software: Includes, but is not limited to, all computer programs and applications, including "shareware." This does not include files created by the individual user.

Temporary File or Permanent File or File: Any electronic document, information, or data residing or located, in whole or in part, whether temporarily or permanently, on the system, including but not limited to spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, or messages.

Email: Messages and other data exchanged electronically between individuals using computers via a computer network and/or an Internet or intranet connection.

342.2 POLICY

It is Department policy that the use of any and all Department computers, software, and electronic systems is subject to approval, review, and inspection by a supervisor or the Department Information Systems staff at any time as outlined below.

342.3 PRIVACY POLICY

Any employee using any computer, electronic storage device or media, Internet service, phone service, information conduit, system, or other wireless service provided by or funded by the Department expressly acknowledges and agrees that the use of such service, whether for business

CATEGORY	DATE ADOPTED	LAST REVIEW	NEXT REVIEW
3	03/31/2015	12/05/2023	12/05/2026

BUENA PARK POLICE DEPARTMENT GENERAL ORDERS

or personal use, shall remove any expectation of privacy the employee, sender, and recipient of any communication using such service might otherwise have, including as to the content of any such communication. The Department also expressly reserves the right to access and audit any and all communications, including content that is sent, received, and/or stored through the use of such service.

342.4 SYSTEM INSPECTION OR REVIEW

An employee's supervisor has the express authority to inspect or review the system, any and all temporary or permanent files, related electronic systems or devices, and any contents thereof when such inspection or review is in the ordinary course of his/her supervisory duties, or based on cause.

When requested by an employee's supervisor, or during the course of regular duties requiring such information, a member(s) of the Department's information systems staff may extract, download, or otherwise obtain any and all temporary or permanent files residing or located in or on the system.

Reasons for inspection or review may include, but are not limited to:

- a) System malfunctions, problems, or general system failure
- b) A lawsuit against the Department involving the employee or related to the employee's duties
- c) An alleged or suspected violation of a Department policy
- d) A need to perform or provide a service when the employee is unavailable

342.5 DEPARTMENT PROPERTY

All information, data, documents, communications, and other entries initiated on, sent to or from, or accessed on any Department computer, or through the Department computer system on any other computer, whether downloaded or transferred from the original Department computer, shall remain the exclusive property of the Department and shall not be available for personal or non-departmental use without the express authorization of an employee's supervisor.

342.6 UNAUTHORIZED USE OF SOFTWARE

Employees shall not copy or duplicate any copyrighted or licensed software, except for a single copy for backup purposes in accordance with the software company's copyright and license agreement. To reduce the risk of computer virus or malicious software infection, employees shall not install any unlicensed or unauthorized software on any Department computer. Employees shall not install personal copies of any software onto any Department computer. Any files or software that an employee finds necessary to upload onto a Department computer or network shall be done only with the approval of the Department's IT Specialist and only after being properly scanned for malicious attachments.

No employee shall knowingly make, acquire, or use unauthorized copies of computer software not licensed to the Department while on Department premises or on a Department computer system. Such unauthorized use of software exposes the Department and involved employees to severe civil and criminal penalties.

CATEGORY	DATE ADOPTED	LAST REVIEW	NEXT REVIEW
3	03/31/2015	12/05/2023	12/05/2026

BUENA PARK POLICE DEPARTMENT GENERAL ORDERS

342.7 PROHIBITED AND INAPPROPRIATE USE / INTERNET USE

Except as noted, access to Department technology resources, including Internet access provided by or through the Department, shall be strictly limited to Department-related business activities. Data stored on, or available through, Department systems shall only be accessed by authorized employees who are engaged in an active investigation, assisting in an active investigation, or who otherwise have a legitimate law enforcement or Department-related business purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

Internet sites containing information that is not appropriate or applicable to Departmental use and that shall not be intentionally accessed include, but are not limited to, adult forums, pornography, chat rooms, and similar or related web sites. Certain exceptions may be permitted with the approval of a supervisor as a function of an assignment.

Downloaded information shall be limited to messages, email, and data files, which shall be subject to audit and review by the Department without notice. No copyrighted and/or unlicensed software program files may be downloaded.

Employees shall report any unauthorized access to the system or suspected intrusion from outside sources (including the Internet) to a supervisor.

Nominal personal use during authorized breaks and lunch periods is allowed, provided that such use does not interfere with the employee's job duties and does not violate any provision of this policy. Examples may include checking and sending personal email and viewing news-related websites.

342.8 PROTECTION OF DEPARTMENT SYSTEMS AND FILES

All employees have a duty to protect the system and related systems and devices from physical and environmental damage, and are responsible for the correct use, operation, care, and maintenance of the system.

Employees are required to maintain and protect their access information, including usernames and passwords. Employees shall not disclose their passwords to others without a specific business purpose. Employees shall not log into the computer system using another member's username and password unless specifically authorized to do so.

It is expressly prohibited for an employee to allow an unauthorized user to access the system at any time or for any reason.

342.9 EMAIL

Email is a communication tool available to employees to enhance efficiency in the performance of job duties. It is to be used in accordance with generally accepted business practices and current law (e.g., California Public Records Act). 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

CATEGORY	DATE ADOPTED	LAST REVIEW	NEXT REVIEW
3	03/31/2015	12/05/2023	12/05/2026

BUENA PARK POLICE DEPARTMENT GENERAL ORDERS

must be confidential, an alternative method to communicate the message should be used.

342.9.1 EMAIL RIGHT OF PRIVACY

Employees using the Department's email system shall have no expectation of privacy concerning communications utilizing the system. 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.

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

342.9.2 PROHIBITED USE OF EMAIL

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing, or any other inappropriate messages on the email system is prohibited and may result in discipline.

Email messages addressed to the entire Department are only to be used for official business-related items that are of particular interest to all users and must be approved by the Chief of Police or a division commander. Personal advertisements are not acceptable.

It is a violation of this policy to transmit a message under another user's name. Users are strongly encouraged to log off the network when their computer is unattended. This added security measure will minimize the misuse of an individual's email, username, and/or password by others.

342.9.3 DISCIPLINE

Any unlawful use of the Department's email system, or use in violation of this policy, may result in discipline up to and including termination. Unlawful use could also result in referral for criminal prosecution.

342.9.4 MANAGEMENT OF EMAIL

E-mail is the primary form of business communication and often includes time-sensitive items. As such, employees shall access and review their email inbox at least once each workday and, at minimum, acknowledge receipt of emails containing messages that require a response, follow-up, or some form of action. Employees shall make every effort to address time-sensitive topics (i.e., something asking for a response or action) in a reasonable period. If an item requires an extended response time, the employee shall advise the sender of the email of an estimated date of completion to the request.

Because the email system is not designed for long-term retention of messages, email that the employee desires to save, or that becomes part of an official record, should be printed and/or stored in another database. Users of email are solely responsible for the management of their mailboxes. Messages should be purged manually by the user at least once per week.

CATEGORY	DATE ADOPTED	LAST REVIEW	NEXT REVIEW
3	03/31/2015	12/05/2023	12/05/2026

BUENA PARK POLICE DEPARTMENT GENERAL ORDERS

342.10 DOCUMENTATION

All employees shall sign the Department Information Access and Disclosure Statement. Employees will be held accountable for this policy and may be disciplined for violations of this, or any policy, regardless if the form is signed or in file.