Live Well. Health Matters.

POLICY TITLE: COMPUTER AND ELECTRONIC MESSAGING
POLICY NUMBER: 3090

COMMITTEE APPROVAL DATE: 11/15/2023 **WRITTEN/REVISED BY**: HUMAN RESOURCES
BOARD APPROVAL DATE: 11/15/2023 **SUPERSEDES:** 01/23/2023

POLICY:

3090 It is the policy of Beach Cities Health District ("District") to establish an environment within the District that encourages open and effective communication and preserves the confidentiality of workplace communications and files created or stored in electronic, magnetic or similar computer related media in order to protect the District's interests and advance its lawful objectives.

3090.1 It is also the policy of the District that computers and software are acquired for the use of employees to advance the mission and service objectives of the District and are operated in compliance with applicable laws and licensing requirements, that procedures relating to the selection and use of software and hardware ensure effective use of District resources and that the District maintain evidence of its right to use multiple copies of software.

SCOPE

3090.2 This policy applies to all personal computers, file servers and peripheral hardware and all software (including local area network hardware and software) whether provided by the District to employees; used by employees in connection with the District's business; or installed on equipment or stored in the District's facilities.

3090.3 This policy also applies to the use of any electronic device or system that creates, stores or transmits messages using the District's computer or telecommunications network including but not limited to e-mail and voice mail ("electronic messaging systems and networks" or "EMS"). This policy does not apply to real time voice transmission over a telephone line. This policy applies to all employees of the District, and any customer, client, independent contractor, volunteer or consultant to the District who is granted access under this policy to an electronic messaging system or network maintained by the District.

3090.4 This policy must be followed in conjunction with other District policies governing appropriate workplace conduct and behavior. Any employee who abuses the District-provided access to e-mail, the Internet, or other electronic communications or networks, including social media, may be denied future access and, if appropriate, be subject to disciplinary action up to and including termination. The District complies with all applicable federal, state and local laws as they concern the employer/employee relationship, and nothing contained herein should be misconstrued to violate any of the rights or responsibilities contained in such laws.

RESPONSIBILITY

3090.5 This policy will be jointly administered by the District's Information Technology (IT) Department and the Human Resources Department. Questions as to the interpretation of this policy will be addressed by the Chief Executive Officer. Questions as to the administration of the District's computer and software programs will be addressed by the Information Technology Manager.

Security and Integrity of the System

3090.5.1 The IT Department is responsible for recommending security procedures and practices designated to prohibit unauthorized access to electronic and magnetic files and records, including, but not limited to password protection, security codes and encryption.

3090.5.2 The IT Department may also review and recommend procedures to protect personal computers from downtime interruption or data loss.

3090.6 It is the responsibility of management to understand, communicate, and enforce this policy uniformly among District employees. It is the responsibility of employees to understand the policies, guidelines, and procedures, and to follow them accordingly. Employees must ask their supervisors if they are unclear as to its application.

CONTENTS

3090.6 Access to Storage Media and Files

All files and data created during the course of employment with the District belong to the District and not to any individual employee. The use of any program that prohibits the District from having access to files, records and information created during the course and scope of employment as an employee of the District, is not permissible. As a general matter, use of security codes or encryption, that cannot be accessed by a system administrator or supervisor violates this policy. Employees who create personal files or store personal data on a District owned memory device such as a hard drive, or disk owned by the District should not expect the District to treat that information differently from other information of a strictly business nature. Employees should have no expectations as to privacy regarding any information and/or data that they may create and/or store on any District owned memory device.

3090.7 Computer Files and Data

3090.7.1 All programs, files, messages and data, whether created, stored, sent or in process on a District computer, are considered to be files and records of the District and will be subject to review and retrieval by representatives of the District whenever the District, in its sole discretion, determines that the District has a need to do so, for any reason not prohibited by law. For example:

3090.7.2.1 When necessary to satisfy a legal obligation or protect an important District right or interest, provided that the information is not more readily available by some other less intrusive means; to perform virus scans or detect intrusion by persons not authorized to use the computer, software or network “hackers”; to perform random audits to ensure compliance with laws and licensing requirements (software audits).

3090.8 Unauthorized Copying

Unauthorized copying of any software whether on a single copy or multiple copy basis is expressly prohibited. Employees may not download District programs from an electronic network or bulletin board outside the District (other than public domain text and graphics files that are not protected by copyright) without authorization of the IT Department. Use of software that is installed on a file server will be monitored by appropriate software monitoring programs to limit

concurrent use to the maximum number of licenses available for each program.

3090.9 Personal Use of District Hardware and Software

Computers, peripheral hardware and software and network hardware and software are made available to employees to assist them in meeting job responsibilities and to advance the mission and service objectives of the District. They are not provided for private or personal use. The District permits incidental, limited personal use of personal computers and software so long as this does not interfere with the intended business purpose of the hardware and software, affect the productivity of the employee, or conflict with any other District policy and procedure for workplace regulation. In limited circumstances the District will provide the necessary hardware, software, or peripheral equipment needed for an employee to work from home. The same expectations apply to an employee's home environment if the District is incurring the expense. Misuse or inappropriate use of hardware, software, or peripheral equipment (such as an internet connection) at an employee's home will be viewed in the same manner as if the employee's set-up was in the office. Anyone who has a "privacy" concern (e.g., an employee desires to use the DSL connection paid for by the District to access personal chat rooms on their personal time) must purchase their own hardware, software, or peripheral equipment. Otherwise, the employee should not have an expectation of privacy since the equipment is owned by the District.

3090.10 Selection, Acquisition and Installation of Software and Hardware

3090.10.1 The IT Department will develop a Software and Hardware Standard listing software programs and hardware that are approved for use with the District. Any product intended for sale, license or commercial distribution outside the District is excluded from this policy. In establishing a Software and Hardware Standard, the IT Department will consult with all managers within the District to determine which software programs are used and are useful to the District, the hardware capabilities of different departments and divisions within the District, and present and future requirements. Software and hardware not included on the Software and Hardware Standard cannot be acquired or installed without an exception to this policy being approved in advance and in writing by the IT Department.

3090.10.2 All software and hardware must be acquired through the District's IT Department. Employees may not purchase software and hardware using a personal credit card, District credit card, or cash and submit for reimbursement for the expense unless justified by an urgent business need and approved by the department head responsible for the user's department. Software cannot be installed on a District computer unless a license agreement and installation media are provided to the IT Department.

3090.10.3 All software and hardware will be installed by the IT Department or by qualified personnel in the user's department after notifying the department head and the IT Department. The IT Department will be designated record holder for network and personal computer software license agreements.

3090.11 Pornography

3090.11.1 Displaying sexually explicit images on District property is a violation of the District's policy on sexual harassment. Employees are not allowed to access, view, download, archive, edit or manipulate sexually explicit material while using the District's resources. If an employee receives material from the outside that is sexually explicit, it is wise to destroy it and advise the sender of the material that you do not wish to receive any additional material

of this nature. The employee should also contact the IT Department for assistance in blocking such content. If the originator of this material is another District employee, the recipient must notify their supervisor immediately and the supervisor will notify Human Resources.

3090.11.2 The intentional viewing or storage of pornography on any system that is owned or has software from the District, whether it is used in the District or at home, is strictly forbidden.

3090.12 Use of Electronic Messaging Systems and Networks (EMS)

3090.12.1 The electronic messaging systems and networks (collectively referred to as the EMS) are made available to employees to assist them in meeting job responsibilities, to advance the mission and service objectives of the District, and not for private or personal use. The District permits incidental, limited personal use of the EMS so long as it does not interfere with the intended business purpose of the EMS, impair the integrity of the EMS or place unusual demands on storage or transmission capacity or conflict with any other District policy or workplace regulation.

3090.12.2 All programs, files, messages and data, whether created, stored, sent or in process on the EMS, are considered to be files and records of the District and will be subject to review and retrieval by representatives of the District whenever the District, in its sole discretion, determines that the District has a need to do so, for any reason not prohibited by law. Employees should have no expectation of privacy regarding any information and/or data created, sent and/or received using the EMS.

3090.12.3 There is no reasonable expectation of privacy in personal messages or information on the EMS. Through inadvertence or as part of the District's normal business procedures, information on the EMS may be subject to disclosure or discovery by the District.

3090.12.4 Information on the EMS may also be accessed and disclosed to third parties if necessary to satisfy a legal obligation or protect an important District right or interest.

3090.12.5 The act of non-compliance with the District policy constitutes misuse. Unacceptable use includes, but is not limited to use of District's electronic messaging facilities:

- for personal profit
- for political purposes
- to interfere with the privacy, security, and legitimate work of others
- to interfere with the performance of the network
- to perform unauthorized copying or transmission of software
- to attempt to violate any connected computer system's security
- to access data being transferred through the network or files on any computer connected to the network without the owner's permission
- to spread computer viruses, Trojan horses, worms or any program designed to violate security, interfere with the proper operation of any computer system, or destroy another user's data
- to transmit "chain letters," unsolicited commercial e-mail (UCE)
- in any manner which violates any federal, state, or local law
- involving the use of a username or account belonging to another individual without their permission

- employing subterfuge to avoid being charged for use of the network or any computer systems attached to it
- for the transmission of material that is harassing or unlawful

3090.13 Message Content and Security

3090.13.1 Communications on the EMS are subject to all other District policies and procedures relating to conduct and communications within the District, including, but not limited to:

3090.13.1.1 District Policy 3070: Use of Mobile Devices
3090.13.1.2 District Policy 3080: Confidentiality
3090.13.1.3 District Policy 3095: Social Media
3090.13.1.4 District Policy 3830: Anti-Harassment
3090.13.1.5 District Policy 3835: Employee Conduct and Working Environment

3090.13.2 Employees should use the same degree of discretion and business judgment in sending messages on the EMS as when sending conventional correspondence or engaging in telephone conversations within and external to the District. This will avoid personal embarrassment and adverse legal consequences for both employees and the District. The IT Department will recommend security procedures and practices to prohibit unauthorized access to information on the EMS. Request for access to another employee's files, messages or data in the EMS that are protected by a personal access code procedure authorized by the Information Technology Manager, must be approved by the Chief Executive Officer.

3090.13.3 Persons not employed by the District such as volunteers, customers, clients, independent contractors or consultants may be given employee-level access to the EMS with prior authorization from the appropriate department head when there is a benefit to the District to be realized by providing this resource to them. Temporary access for individuals who are not bona fide employees of the District must be coordinated with the IT Department.

3090.13.4 All electronic mail correspondence generated from a District email address should include the following message: THE PRECEDING E-MAIL, INCLUDING ANY ATTACHMENTS, CONTAINS INFORMATION THAT MAY BE CONFIDENTIAL, BE PROTECTED BY ATTORNEY CLIENT OR OTHER APPLICABLE PRIVILEGES, OR CONSTITUTE NON-PUBLIC INFORMATION. IT IS INTENDED TO BE CONVEYED ONLY TO THE DESIGNATED RECIPIENT. IF YOU ARE NOT THE INTENDED RECIPIENT OF THIS MESSAGE, PLEASE NOTIFY THE SENDER BY REPLYING TO THIS MESSAGE AND THEN DELETE IT FROM YOUR SYSTEM. USE, DISSEMINATION, DISTRIBUTION, OR REPRODUCTION OF THIS MESSAGE BY UNINTENDED RECIPIENTS IS NOT AUTHORIZED AND MAY BE UNLAWFUL. PLEASE NOTE THAT CORRESPONDENCE WITH THE BEACH CITIES HEALTH DISTRICT, ALONG WITH ALL ATTACHMENTS OR OTHER ITEMS, MAY BE SUBJECT TO DISCLOSURE IN ACCORDANCE WITH THE CALIFORNIA PUBLIC RECORDS ACT. THE BEACH CITIES HEALTH DISTRICT SHALL NOT BE RESPONSIBLE FOR ANY CLAIMS, LOSSES OR DAMAGES RESULTING FROM THE DISCLOSURE OR USE OF ANY INFORMATION, DATA OR OTHER ITEMS THAT MAY BE CONTAINED IN ANY CORRESPONDENCE.

3090.13.5 Failure to comply with this policy may result in disciplinary action up to and including termination from employment.

EXCEPTIONS

3090.14 The Chief Executive Officer is the only person authorized to make exceptions to this policy.