POL.A.04.14 - Records & Data Management Policy

Confidentiality

Certain Park District employees are entrusted with confidential, non-public information. Such employees must access and use such confidential information in a professional manner and in compliance with all Park District policies and procedures and applicable laws.

For the purposes of this Policy, confidential, non-public information, in general, means information relating to Park District employees and patrons that is not generally available to the public. This includes, for example, health-related information, medical documents or insurance numbers, and driver's license numbers.

Park District employees must adhere to the following guidelines with regard to the confidential, non-public information of employees and patrons:

- Do not distribute, disclose or discuss confidential information unless you are authorized to do so, and only to employees with a business need to access the information;
- Avoid, wherever possible, the removal of confidential information from your work area;
- Keep confidential information in secure locations, such as locked cabinets or file rooms. Do not forward confidential information from or to a personal, non-Park District e-mail account; and
- Do not misuse confidential information for personal gain.

Failure to abide by this Policy may result in discipline, up to and including termination of employment.

Records & Data Security

In an effort to protect the District and its users and comply with federal and state laws including the Illinois Identity Protection Act, care must be taken when when handling personal and financial information, including the following:

a. Social Security Numbers. The district shall not require individual's Social Security Number (SSN) to be collected or displayed, unless required by Local, State or Federal government regulations, and must not

- Post or display in any manner an individual's SSN;
- Print a SSN on any document for an individual to access products or services provided by the government;
- Require the transmittal of a SSN number over an unprotected internet connection; or
- Print a SSN number on any materials that are mailed, emailed, or otherwise delivered to the individual.

b. Credit Cards. Federal law sets forth the standards for Payment Card Industry (PCI) compliance to protect cardholder data by limiting the ability of processing software to hold customers credit card information. To ensure PCI compliance, the District partners must a third party processor who must be 100% PCI compliant. All credit card processing and storage of information must be handled by a third party vendor.

c. Passwords. The safety and security of the Park District's computer systems and

resources must be considered at all times. Users may not share any passwords, nor obtain any other users password by any unauthorized means.

Records & Data Retention

The Local Records Commission for the State of Illinois issues regulations establishing procedures for compiling and submitting to the Commission lists and schedules of public records proposed for disposal. The Park District shall comply with any and all requirements of the Illinois Local Records Act and any other statutes, rules or regulations established governing local records retention as well as Park District procedures. Additional guidelines include:

a. Electronic Communications & Data. The Park District provides and maintains messaging agents and electronic facilities including internal and external electronic mail (e-mail) and internet access. Use of these forms of communication is limited to staff, Board, and authorized volunteers. All electronic communications, as well as the equipment and stored information transmitted, received, or archived, are, and remain at all times, the property of the Park District. Accordingly, all messages and files created, sent, received, or stored within the system shall be related to District business and are, and shall remain, the property of the District. No person shall use any electronic communication anonymously or use pseudonyms to attempt to escape from prosecution of laws or regulations, or otherwise escape responsibility for their actions.

Users shall not have any right of personal privacy in any matter stored in, created, received, or sent over the Park District e-mail system. The District reserves the right to retrieve and review any message or file composed, sent or received. It should be noted that although a message or file is deleted or erased, it is still possible to recreate the message. Although electronic mail may allow the use of passwords for security, confidentiality cannot be guaranteed. All electronic messages should therefore be limited to non-confidential matters It is possible for messages to be retrieved and viewed by someone other than the intended recipient. Furthermore, the District may remove or change passwords, as it sees fit. All electronic mail messages sent or received by Commissioners from, or at, any source pertaining to the business of the Park District are “public records” under the Illinois Freedom of Information Act. As such, all messages are available to the public to inspect and copy, subject to the explicit exceptions contained in the law. In order to ensure that such messages comply with this policy, all electronic mail messages are subject to review by authorized Park District staff or authorized Commissioners.

For the protection of the Park District’s computer users, all data, documents, and e-mail messages will be stored on the Park District’s computer network. If the user desires to store documents on diskette, tape, local hard disks, or any other media attached to a personal computer, it is the user’s sole responsibility to make backup copies of the data, documents, or e-mail messages.

Violations of this policy may result in corrective action up to and including termination of employment. If necessary, the District may advise appropriate legal officials of any violations.