CHICAGO PARK DISTRICT
ELECTRONIC COMMUNICATIONS POLICY

1.0 BACKGROUND

1.1 The Chicago Park District ("District") is a unit of local government organized pursuant to 70 ILCS 1505 *et seq*. Because it is a governmental entity, certain records, reports, and other documents possessed or created by the District are open to inspection and copying by the public under the Freedom of Information Act ("FOIA"). It is important to remember that some electronic communications may also be subject to public disclosure under a FOIA request and/or disclosure during litigation.

2.0 POLICY

2.1 The District wishes to promote the responsible and cost-effective use of electronic communications, including but not limited to: electronic mail (*e.g.* "Outlook" or other e-mail programs that may be installed), Internet, Intranet, fax, and voice mail (collectively, "electronic communications") in the furtherance of its business operations. The District is responsible for securing its network and electronic communications system in a reasonable and economically feasible manner against unauthorized access, prohibited uses, abuse, and violation of local, state, federal, and international laws. This responsibility includes informing users of expected standards of conduct and the possible disciplinary actions which may be taken for not adhering to them.

2.2 This document establishes the policies, standards, and procedures ("Policy") for use of District network and electronic communications systems. The District recognizes electronic communications play an increasingly significant role in its business communications. Policies, standards, and procedures must govern usage of internal and external electronic communications in order to: a) assure appropriate use of network and electronic communications systems and related information resources; b) assure effective and cost-efficient use of those systems and resources; c) protect the District from liability; d) comply with local, state, federal, and international laws; e) maintain and protect the District's integrity as a unit of local government; f) maintain public confidence in the District; and g) comport with and advance the District's business interests, policies and mission.

2.3 This Policy and related policies and standards shall govern all internal and external electronic communications made by, on behalf of, or within the District. This Policy applies to all users. Each user is deemed to consent to this policy. The District reserves the right to change or modify this Policy or any related policies or standards at any time, for any reason deemed appropriate by the District.

2.4 This Policy is not a contract or assurance of employment or compensation. This Policy does not create or define any legal rights of District users nor impose any legal duty upon the District.

3.0 POLICY INTENT

3.1 The intent of this Policy is to ensure that all internal and external electronic communications are consistent with the business interests, policies and mission of the District. All electronic communications must comport with the spirit and letter of the District's business interests, policies and mission. This Policy does not attempt to articulate all required or proscribed behavior by users, but merely covers some of the most obvious.

CHICAGO PARK DISTRICT
ELECTRONIC COMMUNICATIONS POLICY

4.0 POLICY APPLICABILITY

4.1 This Policy and related policies and standards apply to all electronic communications and services which are accessed on or from District premises; accessed using District hardware or software, or via on-line access methods paid for by the District; or used in a manner which identifies the individual with the District.

5.0 DEFINITIONS

5.1 LAN/WAN (Local Area Network/Wide Area Network). A network consisting of electronic devices communicating with one another and sharing hardware, software, data, and information resources. Included are all of the communication and computer hardware, operating systems, data, databases, and application software of the District and any stored electronic media and other systems that may be connected or accessed such as electronic mail, Internet, Intranet, fax, on-line services, bulletin boards, and others.

5.2 Wireless Services. A network consisting of electronic devices communicating with one another and sharing hardware, software, data, and information resources outside of the District's LAN/WAN. Included are all of the communication and Mobile Electronic Devices, operating systems, data, databases, and application software of the District and any stored electronic media and other systems that may be connected or accessed such as electronic mail, Internet, Intranet, on-line services, bulletin boards, and others.

5.3 Electronic Communications. Any information in digital electronic format, including, but not limited to electronic mail (*e.g.*, "Outlook" or other e-mail programs that may be installed), voice mail, local databases, externally accessed databases, clip art, digital images, voice and sound recordings, and any digitized information that may be made available on the District's LAN/WAN/Wireless Services. Electronic communications include both internal and external communications.

5.4 Mobile Electronic Devices. Any device issued by the District for work purposes that allows employees to work at varying facilities and outside District-owned facilities. Use of these devices is for the purpose of continued business operations only. Mobile Electronic Devices include, but are not limited to, cell phones, smartphones, broadband cards, pagers, laptops and tablets.

5.5 Authorized Use. Use of District electronic communications hardware, software, databases or on-line services is intended and provided for District business purposes. The District recognizes that an individual may occasionally need to send a personal communication while on the job. As with the telephone, incidental or occasional personal use of e-mail is permitted as long as it does not impact an individual's duties and responsibilities, and as long as the personal use is kept to a minimum. Such personal use is subject to provisions of this Policy.

5.6 Unauthorized Use. Use of the LAN/WAN/Wireless Services for non-District purposes, (except as defined in § 5.3 above) including, but not limited to, entertainment, personal profit, operation of a personal business, commercial or other for profit use, partisan electioneering, lobbying, any violation of local, state, federal, or international law, or any other prohibited use as set forth in this Policy, or as set forth in the future, constitutes unauthorized use and may subject the user to disciplinary action by the District. Unauthorized use may also subject the user to a civil lawsuit, fines, and/or criminal prosecution by appropriate legal or law enforcement authorities. Refer to § § 11 and 12 below.

5.7 Authorized User. An authorized user is a person who has been granted LAN/WAN/Wireless Services access by the District for the District's business purposes. Authorized users may include District employees, its agents, its Board of Commissioners, consultants, vendors, persons who have been contracted to perform certain services for or on behalf of the District under a Professional Services Agreement ("PSA"), and any other person(s) who has been granted access by the District. An authorized user shall be allowed access only to the extent authorized, subject to ongoing compliance with this Policy and any related policies or standards.

5.8 Unauthorized User. An unauthorized user is one who has not been granted LAN/WAN/Wireless Services access by the District. Only those persons who have been authorized to have LAN/WAN/Wireless Services access by the District may use or access the system(s).

6.0 ELECTRONIC COMMUNICATIONS SYSTEMS

6.1 Electronic Communications Systems. Electronic Communications Systems are defined as any service or telecommunications device purchased by the District for use by any employees in the execution of their duties for internal or external communications.

6.2 Telecommunications Devices. Any District owned, supported or issued stationary electronic device (including but not limited to desktops, landlines and printers) or mobile electronic device used by the District in furtherance of its business operations.

6.3 Telecommunications Contract. All employees issued a mobile electronic device must sign and agree to the terms of the Chicago Park District Information Technology Telecommunications Contract. Agreement to the terms of the contract allows the District to release mobile electronic devices and outlines the employee's responsibilities of use.

7.0 WEB-SITES AND HOME PAGES

7.1 The District's Communications Department is solely responsible for reviewing, approving and authorizing any district-related information which is posted on the Internet, including but not limited to each web-site, web-page, and/or home page which represents or purports to represent or is identified with the District, any District Department, any individual Park, or any District or individual Park program(s). Any Department or Park wishing to post information on the Internet must coordinate content with and secure the approval and authorization of the District's Communications Department prior to posting any information on the Internet.

7.2 No user may send a message that purports to make a statement of District policy, either expressly or implicitly, with the exception of messages that quote sections of the Code of the Chicago Park District or other codes, ordinances or policies that have been promulgated by the District.

8.0 USE IS A PRIVILEGE

8.1 Use of the LAN/WAN/Wireless Services and other electronic communication systems is a privilege, not a right. It is not intended that all District employees, consultants, vendors or PSA personnel have or will have access. The District reserves the right to discontinue use, with or without notice or warning, for any reason including, but not limited to, violations of this policy.

CHICAGO PARK DISTRICT
ELECTRONIC COMMUNICATIONS POLICY

9.0 ABSENCE OF PRIVACY

9.1 NO USER SHOULD EXPECT THAT INFORMATION CREATED ON, TRANSFERRED TO, RETRIEVED FROM, OR STORED ON THE LAN/WAN/WIRELESS SERVICES IS PRIVATE, PERSONAL OR CONFIDENTIAL. Documents, files, electronic mail and voice mail created on, transferred to, retrieved from, or stored on District systems and equipment are District property, subject or provisions of applicable law. Electronic communications are subject to audit and review by the District or its authorized agents. In addition, under certain circumstances, electronic communications may be obtained by outside parties in the course of litigation or under a FOIA request. **USERS SHOULD COMPOSE ELECTRONIC MAIL, VOICE MAIL MESSAGES AND OTHER ELECTRONIC COMMUNICATIONS WITH THE KNOWLEDGE THAT THEY ARE BUSINESS DOCUMENTS AND NOT PERSONAL COMMUNICATIONS, THAT THEY MAY BE RETRIEVED AND/OR REVIEWED BY THE DISTRICT, AND THAT THEY MAY IN FACT BECOME PUBLIC OR OTHERWISE BE DISCLOSED UNDER CERTAIN CIRCUMSTANCES**.

10.0 BUSINESS RECORDS

10.1 Information created on, transferred to, retrieved from, or stored on the LAN/WAN/Wireless Services, including but not limited to computer files, electronic mail messages, and voice mail messages may constitute "business records," which may result in legal ramifications similar to the treatment of hard copy documents, even though the information does not exist in hard-copy form, but only in digital form. As a result, such information may be discoverable in litigation and/or may be subject to disclosure under a FOIA request.

10.2 Users should be aware that "deleting" a computer file, electronic mail, or other form of digital document does not necessarily delete the information or document from the system on which it was stored, and that even "deleted" documents may be retrieved. Furthermore, computerized information including electronic mail messages, may be copied by the District as part of routine back-up procedures, may exist in more than one copy or format, and may be stored for certain periods of time. Accordingly, users should exercise sound judgment when transmitting or forwarding electronic communications and should not say anything that would not be said in a hard-copy business document. Users should always think before hitting the "send" key.

11.0 CONFIDENTIALITY AND SYSTEM SECURITY

11.1 No electronic communications system or network is totally secure from breach or tampering by "hackers" or other illegal code-breakers. Users should assume that their electronic communications may not be confidential even if intended to be, and should therefore consider alternate means of transmission for confidential, proprietary or other highly sensitive information or material. Such material or information should be clearly marked to indicate that it is confidential, not for third party use, and not to be forwarded. **Note: Confidential material should never be sent via electronic mail.**

CHICAGO PARK DISTRICT
ELECTRONIC COMMUNICATIONS POLICY

12.0 USER RESPONSIBILITIES AND STANDARDS

12.1 Each user is responsible for adhering to this Policy and all related policies and standards. All users affirm that they understand this Policy and related policies and standards regarding electronic communications, including possible disciplinary action and penalties for violating this Policy or related policies and standards. **USERS AFFIRM THEIR UNDERSTANDING AND ACCEPTANCE OF THIS POLICY AND RELATED POLICIES AND STANDARDS EACH TIME THEY SIGN ON OR LOG ON TO THE DISTRICT'S LAN/WAN/WIRELESS SERVICES**.

12.2 Department Heads are responsible for determining which employees, consultants, individuals engaged under a PSA require access to the District's information network and resources. All supervisors are responsible for ensuring that subordinates and other persons under their supervision adhere to this Policy.

12.3 Users are responsible for respecting and adhering to local, state, federal, and international laws. Any attempt to break those laws through use of the LAN/WAN/Wireless Services may result in litigation against the offender by the proper authorities and/or disciplinary action by the District against the offender. If such an event should occur, the District will fully comply and cooperate with authorities in any investigation and will provide authorities with any information necessary or appropriate.

12.4 Users must comply with all license agreements and policies of networks and on-line services made available on the District's LAN/WAN/Wireless Services. Users must not copy or share any software on the District's LAN/WAN/Wireless Services. **USERS MUST UNDERSTAND THAT THE DISTRICT HAS ZERO TOLERANCE FOR SOFTWARE PIRACY.**

12.5 Users shall not make unauthorized changes to or install unauthorized hardware or software on any component of the LAN/WAN/Wireless Services. Only the District's IT Department or its authorized agents or contractors, may modify or install any hardware or software.

12.6 Any communication sent by users to one or more persons via an electronic network (*e.g.*, electronic mail, Internet, bulletin board, social media or other on-line service) is identifiable and attributable to the District, and might be legally imputed to the District. Therefore, users must not send any electronic communication that exceeds the scope of their duties and authority.

12.7 Users must not make any statement – exculpatory or not – or conduct any activity that may give rise to any liability on the part of the District, and must be careful not to make any statement that may bind the District to a contract without prior authorization to do so.

12.8 Users must not disclose confidential or proprietary information to unauthorized persons or parties without express authorization by the Department Head to do so.

12.9 Authorized users must not permit unauthorized use under their passwords, authorization codes, IDs or accounts. Under no circumstances may another employee, friend, co-worker, family member, park patron, entity or organization access or use the District's LAN/WAN/Wireless Services under an authorized user's ID, password, authorization code or account.

12.10 Authorized users must keep their passwords, authorization codes and IDs private, but must provide them to the District when requested. Accounts, passwords, authorization codes or IDs are not to be shared.

12.11 All electronic communications should be handled in an efficient, business-like and cost-effective manner. Appropriate judgment and discretion should be used whenever sending electronic communications. Users must not unnecessarily tie up the District's electronic communication networks and systems and should be respectful of other users' needs to utilize the systems. Uses such as "chat rooms" are not considered appropriate uses of the District's LAN/WAN/Wireless Services.

13.0 PROHIBITED USES

13.1 In general, any use which violates this Policy or related policies and standards, breaks or attempts to break any local, state, federal or international law(s), including but not limited to trademark, copyright, license or patent infringement, or contravenes the District's Equal Employment Opportunity, Affirmative Action, Sexual Harassment, or other policies is prohibited. The following prohibitions are not all inclusive, but merely represent some of the most obvious prohibited uses of the District's electronic communications and services.

13.2 It is prohibited to use any electronic communication or communications system in any manner that would discriminate against any person on the basis of sex, race, ethnicity, national origin, age, disability, sexual orientation, religion, political beliefs, or any other characteristic prohibited by law or that is contrary to the letter or spirit of the District's Equal Employment Opportunity and Sexual Harassment policies.

13.3 It is prohibited to use electronic communications and services to knowingly transmit, retrieve, download, up-load or store any communications which are: discriminatory or harassing to any individual or group; derogatory to any individual or group; obscene, pornographic, indecent, profane, or sexually-explicit; or defamatory, libelous or threatening to any individual or group.

13.4 It is prohibited to use electronic communications and services for non-work-related uses including but not limited to: gambling, "chain letter", solicitation "junk mail", games, personal entertainment, personal financial gain, personal electronic trading, personal business operation, commercial product advertisement or endorsement, partisan political purposes, lobbying, fund-raisers, or religious activities.

13.5 It is prohibited to use electronic communications and services for any purpose which: infringes on third party copyrights, trademarks, trade secrets, license agreements, patents or other intellectual property rights; violates or attempts to violate any applicable law, regulation, license or policy, or for any other purpose which is illegal or against District policies or contrary to the District's interests. **IT IS PROHIBITED TO COPY OR PIRATE ANY SOFTWARE OR TO USE OR INSTALL ANY PIRATED OR UNAUTHORIZED SOFTWARE OR HARDWARE ON THE DISTRICT'S LAN/WAN**.

13.6 It is prohibited to create a personal web-site, web-page, or home page on the District's LAN/WAN/Wireless Services.

13.7 It is prohibited to post any information on the Internet or to create or post a District, District Department or individual Park web-site, web-page, or home page **without prior approval and express authorization of the District's Communications Department.**

13.8 It is prohibited to use encryption technology in connection with the LAN/WAN/Wireless Services unless expressly authorized by the District.

13.9 It is prohibited to forge any electronic communication or to forward any communication that attempts to hide or alter the identity of the sender/forwarder or represents the sender/forwarder as someone else.

13.10 It is prohibited to attempt to "hack" into other systems, "crack" passwords, or otherwise breach computer or network security measures.

13.11 It is prohibited to monitor electronic communications of other users or third parties except under explicit authorization of District management and only for legitimate purposes including audit and review.

13.12 It is prohibited to intentionally spread computer viruses or to create or spread programs that harass or annoy others, or that damage, tie-up, or alter District software or hardware.

14.0 COMPLIANCE

14.1 Audit and Review. The District reserves the right to access, audit, review, delete, disclose or use all electronic communications, including any digitized information that may be made available on the LAN/WAN/Wireless Services, and other information stored or transferred on District systems at any time without notice and without recourse regardless of the content of the information, subject to a finding of probable cause that a violation has occurred as determined by the Inspector General or his/her designee.

14.2 Consent. Use of the District's electronic communications network and related systems constitutes each user's consent to such access, audit, review, deletion, disclosure or other use by the District. Upon request, a user shall reveal to the District all passwords, IDs or other codes necessary to access the user's files, directory(ies), account(s), electronic mail, or voice mail.

14.3 Disciplinary Action for Violation. Violation of this Policy or any related policies or standards may be grounds for disciplinary action up to and including termination of employment of employees, or termination of the contract(s) and/or services of an outside consultant, vendor, or party under a PSA with the District, regardless of whether the user was an authorized user or not. In addition, some violations may result in restitution, civil liability and/or criminal prosecution by appropriate authorities.

14.4 Reporting Unauthorized Use. Authorized users must report any violations or suspected violations of this Policy or any related policies or standards to their supervisor, Department Head, Human Resources Department, Region Manager, or IT Department as soon as they become aware of it.

14.5 Inquiries and Questions about Electronic Communications. Any inquiries, questions or concerns relating to use of electronic communications should be directed to the District's IT Department.

14.6 Procedure for Review. Notwithstanding the forgoing, the District may only access electronic communications subject to this Policy if there exists probable cause that a violation of this Policy has occurred. Procedurally, the District must first refer reasonable allegations of violations of this Policy to the Inspector General or his/her designee for the express purpose of determining whether or not probable cause exists. If probable cause is found, the Inspector General shall notify the District so that disciplinary and/or legal action may be taken pursuant to this Policy.

CHICAGO PARK DISTRICT
ELECTRONIC COMMUNICATIONS POLICY

STATEMENT OF USER COMPLIANCE

I have read and understood the CHICAGO PARK DISTRICT ELECTRONIC COMMUNICATIONS POLICY/J050702T. I understand that violation of this Policy may lead to disciplinary action, up to and including termination of employment or termination of contract, civil fines and/or criminal prosecution. By signing below, I agree to adhere to the policy and related policies and standards. I understand that this Policy is not a contract or assurance of employment or compensation. I understand that this Policy does not create or define any legal rights of District employees nor impose a legal duty upon the District.

THIS DOCUMENT WILL BE PLACED IN YOUR PERSONNEL FILE

Signature: _____

Name (print):_____

Employee Number: _____

Job Title: _____

Date: _____