05.20.00. POLICY STATEMENT

This Electronic Communications and Technology Use Policy ("Policy") is intended to govern, and provide guidance with respect to, the use of Electronic Communications equipment and systems including, but not limited to, electronic mail (*e.g.,* "Outlook" or other e-mail programs that may be installed), the Internet, Intranet, fax, and voice mail (collectively, "Electronic Communications") and various other technology resources such as computer software, computers, laptops, electronic notebooks, cell phones, smart phones and printers ("Technology Resources") purchased, leased, owned or otherwise controlled by the Forest Preserve District of Cook County (the "District").

05.20.01. PURPOSE

The District wishes to promote the responsible and cost-effective use of Electronic Communications and Technology Resources in the furtherance of its business operations. The District is responsible for securing its network, Electronic Communications, and Technology Resources 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 that may result from not adhering to the same.

05.20.02. REFERENCES

Cook County Rules & Regulations
(Rules of Conduct: Pages 20-23)

Forest Preserve District of Cook County, Employee Handbook
(Use of District Property Section: Page 17)

Forest Preserve District of Cook County, Employee Handbook
(Rules of Conduct Section: Pages 20-23)

05.20.03. DEFINITIONS

N/A

05.20.04. SCOPE

This document establishes the policies, standards, and procedures to ensure that employees understand the guidelines governing the use of Electronic Communications and other Technology Resources. This Policy governs usage of internal and external Electronic Communications and Technology Resources in order to: **a)** assure appropriate use of network and electronic communication 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)** advance the District's business interests, policies and mission.

This Policy and related policies and standards shall govern all internal and external Electronic Communications and Technology Use by, on behalf of, or within the District.

This Policy applies to all employees and Users (collectively, "User" or "Users"). By signing the attached acknowledgement each User is deemed to have received, read, understood, acknowledged, and agreed 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, at the absolute discretion of the District.

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

This Policy does not cover every possible situation. Rather, it is designed to express the District's philosophy and set out the general principles that employees should apply when using electronic communications or technology resources.

05.20.05. RESPONSIBILITY

The Information Technology Department: The Information Technology (IT) Department shall be responsible for ensuring employee compliance with this policy.

Supervisors: Supervisors shall be responsible for: **(1)** Periodically reminding employees about this policy, or when and where appropriate; **(2)** Returning technology related devices (such as laptops, tablets, and mobile phones) to the IT Department prior to, or after, a District employee leaves District employment, or at the request of the IT Department.

Human Resources Department: The Human Resources Department is responsible for: **(1)** informing the Information Technology Department when a District employee is off-boarding, or has off-boarded; and, **(2)** informing the Information Technology Department prior to the on-boarding of a District employee.

District Employees: All District employees are required to comply with this policy.

05.20.06 PROCEDURES

Authorized Use:

1.0 Use of District Electronic Communications, hardware, software, databases or on-line services, or other Technology Resources are intended and provided for District business purposes only. The District recognizes that an individual may occasionally need to send a personal communication while on the job. Limited personal use of the telephone, e-mail and electronic devices is permitted as long as it does not impact an individual's duties, responsibilities and the personal use is kept at a minimum. Such personal use is subject to the provisions of this Policy. However, it is strongly recommended that Users simply do not use District equipment

and systems for personal reasons. In addition, any personal files and/or information that are stored on District systems (PCs, laptops, phones, etc.) are considered property of the District and are subject to this Policy.

Unauthorized Use:

1.1 Use of the District network or other Technology Resources for non- District purposes (except as defined in Section 1.1 above) including, but not limited to, entertainment, personal profit, operation of a personal business, commercial or other for profit use, partisan electioneering or other political activities, 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 up to and including termination of employment with 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 Sections 9 and 10 below.

General:

2.0 The District provides employees with personal computers, laptops, printers, cell phones, smart phones and other Technology Resources as necessary to perform their duties. In general, equipment is selected based on its suitability for a particular business purpose.

2.1 The District encourages the use of Electronic Communications and Technology Resources because such tools often make communication, research and other business functions more efficient and effective. In addition, Electronic Communications and some Technology Resources can provide valuable sources of information about vendors, customers, technology, and new products and services. Everyone connected to the organization, however, should remember that electronic media and services provided by the District are the property of the District, are public record, and subject to Freedom of Information Act requests, and their purpose is to facilitate and support District business.

2.2 Further, all forms of chain mail (including virus warnings, "good luck" and similar messages) are unacceptable. The transmission and sharing of user names, passwords internally, externally or other information related to the security of District computers is not permitted.

2.3 This Policy does not cover "best practice" for email use in detail, but Users should avoid sending unnecessary informational emails to large parts of the organization.

External Email and Participation in Online Forums:

3.0 Users should be aware that any messages or information sent using the District systems may be identifiable and attributable to the District. An email carries the same weight in law as a letter written on District letterhead or stationery.

3.1 Employees Users should note that even with a disclaimer, a connection with the District exists and a statement could be imputed to the District. Therefore, no one should rely on disclaimers as a way of insulating the District from the comments and opinions that are contributed to forums. Instead, discussions must be limited to matters of fact while using District systems or a District provided account. Communications must not reveal information about District

processes, techniques, trade or confidential information and must not otherwise violate these or other District policies.

Physical Security and Care of District Issued Equipment:

4.0 Users with District technology devices, including, but limited to, portable (laptop) computers must take reasonable precautions. When out of the office, the computer should always be under direct control of the User.

4.1 Users are responsible for general care of all equipment issued by the District. The IT department should be informed of any broken devices immediately, at which time corrective instructions will be given.

4.2 Upon resignation or termination, District employees are responsible for the return of all assigned mobile equipment and devices to the IT department. That includes laptops, tablets, cell phones and/or any other equipment issued by the District.

Privacy:

5.0 Users should have no expectation of privacy while using District equipment or communication devices.

5.1 The District has the ability to routinely gather logs for most electronic activities. For example, telephone numbers dialed, call length, and time at which calls are made are recorded for the following purposes:

- Cost analysis
- Resource allocation
- Optimum technical management of information resources

5.2 The District reserves the right, at its discretion, to review any electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other District policies. This includes the use of spot checks on the Internet (Web) use, network files and email without prior notification.

5.3 Software tools to identify possible breaches of this Policy (e.g., highlighting access to websites with unacceptable content or emails containing abusive language) may be used. The results will be reported to the District management and thoroughly investigated where appropriate. It should not be assumed that internal or external Electronic Communications are totally private. Accordingly, particularly sensitive or personal information should be transmitted by other means.

File Storage:

6.0 The IT support group creates backup of all email and network file storage every night. This data is retained in a secure location and can be used in the event of:

- Accidental deletion of important material
- A "disaster" necessitating complete recovery of one or more of the District systems.

6.1 Data and other files created or modified should be stored within the network. This would be comprised of a shared or the user's individual assigned network location.

6.2 It is particularly important that users of portable computers routinely make copies of key documents, either by copying them to the network when in the office, or to USB disk when away from the office. It is the laptop user's responsibility to ensure that this is done correctly. The IT support group is not responsible for backing up data saved to local drives or on portable devices.

Contract/Part-Time/Seasonal/Volunteer Staff:

7.0 The District may provide independent contractors, consultants, volunteers, temporary employees, part-time employees, and seasonal employees ("User" or "Users") with access to Electronic Communications and Technology Resources for the sole purpose of fulfilling their designated or contractual role with the District. No personal use by these Users of Electronic Communication and Technology Resources provided by the District is permitted at any time.

Viruses and Malware:

8.0 All computer viruses and malware must be reported immediately to the IT support group. The IT support group is responsible for updating virus detection software from time to time and providing detailed guidelines in the event of a major problem. The IT support group will also investigate any infection and must receive the full cooperation of all employees and other Users in attempting to identify the source.

User Responsibilities and Standards:

9.0 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 policy and standards regarding Electronic Communications and Technology Resources, including possible disciplinary action and penalties for violating this Policy or related policy and standards. In addition to signing the acknowledgement form, **EMPLOYEES AND USERS AFFIRM, RESPECTIVELY, THEIR UNDERSTANDING AND ACCEPTANCE OF THIS POLICY AND RELATED POLICIES AND STANDARDS EACH TIME THEY SIGN IN OR LOG ON TO THE DISTRICT NETWORK.**

9.1 Department Heads are responsible for determining which Users and employees of the District are allowed access to the District information network resources. All supervisors are responsible for ensuring that subordinates and other persons under their supervision adhere to this Policy.

9.2 Users are responsible for respecting and adhering to local, state, federal, and international laws, as well as applicable Cook County and District policies. Any attempt to break those laws or violate such policies through use of the network 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.

9.3 Users must comply with all license agreements and policies of networks, and on-line services made available on the District network. Users must not copy or share any software on the District network. **EMPLOYEES AND USERS, RESPECTIVELY, UNDERSTAND**

AND ACKNOWLEDGE THAT THE DISTRICT HAS ADOPTED A ZERO-TOLERANCE POLICY FOR SOFTWARE PIRACY.

9.4 Users shall not make unauthorized changes to, or install, unauthorized hardware or software on any component of the network. Only the District IT Department or its authorized agents or contractors may modify or install any hardware or software. Employees and Users shall not access any external networks or information resources or utilize any District resources without proper authorization.

9.5 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.

9.6 Users must not disclose confidential or proprietary information to unauthorized persons or parties without express authorization to do so.

9.7 Authorized Users must not permit unauthorized Users access under their passwords, authorization codes, IDs or accounts. Under no circumstances may another employee, friend, co-worker, family member, park patron, and entity or organization access or use the District network under another authorized user's ID, password, authorization code or account.

9.8 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. No User has authority to delegate authorized use to another User except under authorization by the General Superintendent.

9.9 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 electronic communication networks and systems and should be respectful of other users' needs to utilize the systems. Uses such as "chat rooms" are not typically considered appropriate uses of the District network.

Prohibited Uses:

10.0 In general, any use that violates this Policy or related policy 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 laws, or contravenes the District 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 District Electronic Communications and services.**

10.1 It is prohibited to use any Electronic Communications or Technology Resources in any manner that could 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 Equal Employment Opportunity and Sexual Harassment policies.

10.2 It is prohibited to use Electronic Communications or Technology Resources to knowingly transmit, retrieve, down-load, up-load or store any communications that 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.

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

10.4 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 interests.

10.5 It is prohibited to create a personal web-site, web-page, or home page on the District network.

10.6 It is prohibited to use encryption technology in connection with the network unless expressly authorized by the District.

10.7 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 represent the sender/forwarder as someone else.

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

10.9 It is prohibited to monitor Electronic Communications of other users or third parties except under explicit authorization of the General Superintendent and only for legitimate purposes, including audit and review.

Compliance:

11.0 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 network, and other information stored or transferred on District systems at any time without notice and without recourse regardless of the information contents, subject only to provision of applicable law.

11.1 Disciplinary Action for Violation. Violation of this Policy or any related policies or standards may be grounds for corrective action up to and including termination of employment of employees, or termination of the contract(s) and/or relationship of an outside User with the District, regardless of whether the User was an authorized User or not. In addition, some violations may result in civil liability and/or criminal prosecution by appropriate authorities.

11.2 Reporting Unauthorized Use. Authorized employees and/or 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, or IT Department as soon as they become aware of it.

11.3 Inquiries and Questions about Communication performed on the District Network. Concerns relating to using of any electronic media should be directed to the District IT Department.

05.20.07. TRAINING REQUIREMENTS

N/A

05.20.08. ACTION PLAN TO COMMUNICATE/DISSEMINATE

1. This policy should be distributed to all staff.

2. This policy should be added to the District shared drive, intranet, and website.

3. Department Heads should work to ensure that their staff are knowledgeable about this policy.

If you have questions, comments, or suggestions concerning District policies, please contact:

Forest Preserve District of Cook County
Office of the General Superintendent
Attn: Anthony D. Tindall, Policy Director
69 W. Washington St., Suite 2040, Chicago, IL 60602
Office: (312) 603-8351; Email: Anthony.Tindall@cookcountyil.gov

Appendix A:
Employee User Agreement

I hereby certify that I have received, read, understand and agree to all of the terms and conditions of the Forest Preserve District of Cook County (the "District") Electronic Communications & Technology Use Policy. I also understand that the laptop computer, tablet, and other related technology or equipment I am being issued is the property of the District. I will return the laptop computer and/or tablet and any other related equipment I am issued in the same condition in which I receive it, excluding normal wear and tear and unforeseen system breakdowns, i.e. hard drive failure, etc. I understand that I must notify the Technology Department immediately should the equipment or technology I am assigned becomes damaged or lost.

Employee Name: _____

Employee Job Title: _____

Employee Phone Number: _____

Employee Department: _____

Employee Signature: _____ **Signature Date:** _____

Technology Department Use Only	
Technology/Equipment Type:	
Carrying Case (Yes or No):	
Power Supply & Cord (Yes or No):	
Serial Number#	
Asset Tag#	
Other Number#	
Other Number#	
CFO/ Designee Name:	
CFO/ Designee Signature:	
Date:	
Other Notes:	