Lake County Forest Preserves

General Offices
1899 West Winchester Road
Libertyville, Illinois 60048
847-367-6640 • Fax: 847-367-6649
www.LCFPD.org

DATE: November 7, 2024

MEMO TO: Gina Roberts, Chair
Finance Committee

FROM: Mary E. Kann
Director of Administration

RECOMMENDATION: Approve amendments to the Procedures sections of Personnel Policies 2.4 – Personnel Recruitment, 6.1 – Promotions and Transfers, 8.7 – Harassment, and 8.10 – End User Account.

STRATEGIC DIRECTION SUPPORTED: Leadership

FINANCIAL DATA: There is no immediate direct financial impact to these changes.

BACKGROUND: From time to time, the District amends its Personnel Procedures. Staff recommends the attached changes to Sections 2, 6 and 8 of the Personnel Procedures, which include the following changes:

- 2.4 – Personnel Recruitment: Amends the procedure to require an employee to complete their introductory period before applying for a promotion.

- 6.1 – Promotions and Transfers: Amends the procedure to require an employee to complete their introductory period before applying for a promotion.

- 8.7 – Harassment: Effective January 1, 2025, amends the procedure to be compliant with legislative changes. These changes include the addition of "family responsibilities" and "reproductive health decisions" as protected classes. It also changes the timeframe to file a charge of discrimination with the Illinois Department of Human Rights from 300 days to 2 years from the date of occurrence.

- 8.10 – End User Account: Amends the procedure to specifically outline expectations surrounding the use and retention of e-mail and training expectations.

Therefore, it is the recommendation of staff that the attached changes to the Procedures sections of Personnel Policies 2.4 – Personnel Recruitment, 6.1 – Promotions and Transfers, 8.7 – Harassment, and 8.10 End User Account be approved.

REVIEW BY OTHERS: Director of Finance, Chief Information Officer, Deputy Director of Human Resources & Risk, Manager of Board Operations, Corporate Counsel.

MOTION: Motion to amend the Procedures sections of Personnel Policies 2.4 – Personnel Recruitment, 6.1 – Promotions and Transfers, 8.7 – Harassment, and 8.10 – End User Account, in the forms attached to staff's memo dated November 7, 2024, with such amendments to become effective immediately, except for the amendments to Section 8.7 – Harassment, which will take effect on January 1, 2025.

APPROVAL:

Date:_____ ☐ Roll Call Vote: Ayes: ____ Nays: ____

☐ Voice Vote Majority Ayes; Nays: ____

2.4 Personnel Recruitment Procedures

Effective Date: August 15, 1980
Revision Date: May 27, 1994, November 7, 2013, May 4, 2023, February 8, 2024, November 7, 2024

Procedure

1. The Department Director must notify the Director of Administration of the need to fill a vacancy and complete the position opening process through the applicant tracking system.

2. To ensure that the policy of Equal Employment Opportunity is part of the recruitment process the Human Resources Division will prepare an Employment Opportunity Notice and post the notice in selected locations throughout the County and internally at various District facilities. Human Resources will notify the State Employment Service of position vacancies.

3. If an employee from another department is selected to fill the vacancy, at least two (2) weeks' notice will be given to the Director of the transferring employee. Arrangements for an adequate transition period shall be made to avoid a serious disruption of work.

4. The Human Resources Division will place advertising in the media for position vacancies. If a similar position becomes vacant within six months of a recruitment, or one year for Ranger Police positions, applications received for the first recruitment may be considered to fill the position without recruiting additional candidates with approval of the Director of Administration.

5. In difficult recruitment markets, the Director of Administration may, with the concurrence of the Executive Director 1) designate a referral bonus to be paid to existing employees for a successful new employee referral and 2) designate a signing bonus for prospective employees. The application of any referral or signing bonus must be reviewed annually.

6. Employment agencies may be utilized for recruitment if authorized by the Executive Director.

7. All applicants for employment will be referred to the Administration Department. If there is an opening for a position in which the applicant is interested, they may complete an employment application. All application materials including cover letters and resumes, must be submitted online through the District's Applicant Tracking System.

9. Current employees wishing to apply for an externally posted vacancy must apply through the District's Online Applicant Tracking System.

10. Current employees must have completed their introductory period with the District in order to be considered for a different District position, unless for purposes of a reasonable accommodation.

6.1 Promotions and Transfers

Effective Date: August 15, 1980
Revision Date: September 16, 1994, June 21, 2002, November 12, 2013, July 1, 2021, November 7, 2024

Procedure

It is the responsibility of the Administration Department and the Department Director to fill job openings with the best qualified people.

1. The District may, at its discretion, initiate the transfer or promotion of an employee.

2. An employee desiring a transfer to an open position of the same job title must submit a written request for transfer to the appropriate Department Director and the Manager of Human Resources and Risk.

3. An employee interested in promotion to an open position must apply according to the application instructions for the posted position. An employee must have completed their introductory period with the District in order to be considered for a different District position, unless for purposes of a reasonable accommodation.

4. When an employee is transferred or promoted to a different position all accrued benefits remain with the employee. A promoted employee will be paid as stipulated in Section 5.2

5. An employee transferred or promoted to another department will give the current Department Director two (2) weeks notice from the date the position is accepted.

8.7 Harassment

Effective Date: April 15, 1983
Revision Date: June 19, 1987, April 21, 1995, May 19, 2000, June 21, 2002, October 14, 2005, April 9, 2013, December 7, 2017, March 8, 2018, January 10, 2019, February 11, 2020, October 5, 2020, May 10, 2023, January 1, 2025

Procedure

If an employee believes that they have been harassed sexually or otherwise, they should report the incident(s) immediately to a Manager or Director. The District will take all reasonable steps to assure that any harassment that may be determined to exist will be eliminated.

Sexual harassment according to the federal and state law is defined as:

> Any unwelcome sexual advances or requests for sexual favors or any conduct of a sexual nature when (1) submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment, (2) submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual, or (3) such conduct has the purpose or effect of substantially interfering with an individual's work performance or creating an intimidating, hostile or offensive work environment.

Specific behaviors that the District will consider sexual harassment include but are not limited to the following:

1. Unwelcome sexual jokes, pressuring a subordinate to go out on a date, sexual innuendos, gender-specific insults, inappropriate references to anatomy, or threats whether spoken or written.
2. Suggestive or insulting sounds, (e.g. whistling, "catcalls,") or suggestive bodily gestures.
3. Showing or displaying pornographic or sexually explicit objects, pictures or other materials in the workplace
4. Unwelcome touching, hugging, kissing, pinching or intentionally brushing the body; coerced sexual conduct; or actual assault.
5. Any statement or action indicating that job status, compensation, job assignments, or other conditions of employment are dependent upon granting or refusing sexual favors.

Other protected classes:
Race
Disability
Age
National origin
Sex

Religion
Marital status
Gender Identity
Pregnancy
Sexual orientation
Order of Protection status
Family Responsibilities
Reproductive Health Decisions

Specific behaviors that the District will consider harassment based on a protected status include but are not limited to the following:

1. Making offensive slurs, epithets or jokes based on any of the above protected classes;
2. Circulating offensive literature or other biased printed material; or
3. Otherwise creating an environment that is hostile to a worker or workers based on the above protected classes.

Bullying:
Workplace bullying by District employees is a form of harassment. District employees shall not engage in workplace bullying, which includes but is not limited to:

- Oral or written (including by electronic means) bullying, which includes but is not limited to, oral or written statements by a District employee to another District employee that (i) defame, ridicule, or malign the latter employee or their family; (ii) include persistent name-calling that is hurtful, insulting, or humiliating to the latter employee; (iii) use the latter employee as a target of jokes; or (iv) include abusive remarks toward the latter employee.
- Gesture bullying, which includes non-verbal threatening or harassing gestures made by a District employee toward another District employee.
- Exclusion: socially or physically excluding or disregarding a person in work-related activities for non-work-related reasons.

Any District employee, who believes they have been harassed, or observes an incident of harassment, must promptly report it to a supervisor, who shall report it to the Director of Administration. If the employee does not feel that the incident can be discussed with their direct supervisor, the incident should be reported to the Department Director or the Director of Administration. All incidents or complaints of harassment must be reported even in the event the employee does not want to make a formal complaint. The employee may also contact Human Resources, the Inspector General or the Illinois Department of Human Rights.

The employee should contact the Director of Administration if they are not satisfied with the way the report of harassment has been handled. Employees may report harassment and raise concerns without fear

of reprisal. The District will not tolerate any retaliation against an employee for filing a sexual or other harassment complaint. Employees who report harassment are protected under the Illinois Administrative Procedure Act, the Whistleblower Act and the Illinois Human Rights Act.

Upon receipt of the complaint, the District shall take prompt, thorough and impartial steps to investigate the complaint. Following the investigation of the complaint, which will be commenced immediately unless clear evidence makes an investigation unnecessary, the District will weigh the facts and decide on the validity of the complaint. If the complaint is determined to be valid, the offender will face immediate and appropriate disciplinary action based on the severity of the incident. Disciplinary action may include warnings, suspensions, discharge or demotion.

The District is committed to responding to harassment complaints in a prompt and fair manner. It is hoped that complaints of harassment can be resolved within the District. However, an employee may also contact the Illinois Department of Human Rights (IDHR) and the Equal Employment Opportunity Commission (EEOC) about filing a formal charge; the Director of Administration can provide an employee with information on how to contact these agencies. In addition, the addresses of these agencies are listed on the attachment to this policy. The IDHR charge must be filed within ~~300 days~~two (2) years of the alleged offense. A complaint with the EEOC must be filed within 300 days. These deadlines may be extended for continuing offenses under law. In addition, an appeal process is available through the Illinois Human Rights Commission (IHRC) after the IDHR has completed its investigation of the complaint. Where the employing entity has an effective sexual harassment policy in place and the complaining employee fails to take advantage of that policy and allow the employer an opportunity to address the problem, such an employee may, in certain cases, lose the right to further pursue the claim against the employer. An employee who feels that they have been retaliated against after filing a charge with the IDHR or EEOC has 300 days from the alleged retaliation to file a retaliation charge.

An employee who has been physically harassed or threatened while on the job may also have grounds for criminal charges, such as assault or battery.

FALSE AND FRIVOLOUS COMPLAINTS

Given the seriousness of the consequences for the accused, a false and frivolous charge of harassment is a major offense that can itself result in disciplinary action up to and including discharge. False and frivolous complaints are cases where the accuser is using a harassment complaint to accomplish some end other than stopping the harassment. It does not refer to charges made in good faith that cannot be proven.

ADMINISTRATIVE CONTACTS

Illinois Department of Human Rights
100 West Randolph Street
Suite 10-100
Chicago, IL 60601

Equal Employment Opportunity Commission
500 West Madison
Suite 2800
Chicago, IL 60661

Tel. : 312-814-6200 Tel : 800-669-4000

Illinois Human Rights Commission
100 West Randolph Street
Suite 5-100
Chicago, IL 60601
Tel. : 312-814-6269

If the above contact information changes, the Director of Administration will promptly notify employees via e-mail or other means.

8.10 End User Account

Effective Date: November 12, 2013
Revision Date: June 28, 2018, May 10, 2023, November 7, 2024

Procedure

A. General

An "account" consists of the user's ID required for the user to do business. Each user account will be created using the employee's preferred name.

B. Termination of Accounts

A user's access to their account(s) must be terminated as soon as practical but no later than 3 days after separation from employment. An email account may be forwarded to an alternate District employee as recipient of this email. All requests for a temporary extension of this deadline, or any other exception to this policy, must be made in writing to IT and be approved by the Chief Information Officer (CIO) or designee. The District in any case will not forward email to accounts outside the District Network.

C. Change Notice

Accounts are issued because authorized access to resources is required. If the user's needs or responsibilities change, IT must be notified by the supervisor. It is the supervisor's responsibility to report changes in responsibilities and authorization requirements to the IT two weeks prior to the change. Changes should be requested via the Electronic HelpDesk System. Account termination or reactivation requests will only be accepted from a supervisor or Human Resources. A user cannot request changes to their own account.

D. Account Inactivity

IT maintains log files of access to most resources. If an account shows no activity for three months, it may be disabled. The user must contact the IT Help Desk to reactivate it. An account that has been idle for six months will be removed without notice.

E. Network Password

Passwords are an important aspect of information security. They are the front line of protection for user accounts and other forms of access. A poorly chosen password can result in the compromise of the District's network. As such, all users are responsible for taking the appropriate steps to select and secure their passwords.

F. Account Abuse

Log files may be scanned by IT for indications of inappropriate use and/or resource abuse, for which an account can be terminated without notice. Examples of Account Abuse include, but are not limited to:

- **Theft and Vandalism**
  Theft and vandalism of network resources/computer systems and peripherals will be handled by the appropriate authorities (Ranger Police and/or appropriate law enforcement agencies). The District will pursue and support criminal prosecution of individuals suspected of theft and/or vandalism.

- **Unauthorized Use of Network Services**
  Any individual for whom an active account does not exist, and is determined to be using any network services, will be referred to the appropriate authorities including the CIO, Director of Administration and the appropriate Department Director. Incidents of unauthorized use that involve individuals not directly associated with the District will be handled by the appropriate law enforcement agency. If expenses are incurred by the District during unauthorized use (i.e., paper, printer supplies, etc.), the District reserves the right to pursue full reimbursement of those costs from the individual.

  Use of restricted network services without authorization is considered an abuse of privilege and may result in restriction, denial of network access, and where appropriate disciplinary action. Current restricted-use network resources include printers reserved for use by an individual, department or group, and workstations and servers that have restricted login access.

- **Unauthorized access to accounts**
  Any attempt to gain access or to use an account other than by the owner will be considered a severe violation of network policy and will be cause for discipline, up to and including discharge. Such attempts include, but are not limited to, gaining access to a user's account while the user is away from a workstation or efforts to determine another user's password by closely watching a login. Possession of tools that can be used to subvert security is grounds for account suspension.

- **Cracking passwords**

Any attempt to crack or otherwise obtain passwords is prohibited, and will be cause for discipline, up to and including discharge. Storing or transferring unencrypted password information is prohibited. Writing, transferring, compiling or running programs designed to guess passwords or otherwise gain unauthorized access to user or system accounts or passwords are generally prohibited. This includes programs or techniques designed to trick users into divulging their passwords. The CIO is the only employee who may possess and utilize Password Recovery Software, to be used in the case of a Director needing access to a password protected file.

- **Sharing accounts**
  An account is assigned to an individual. This individual is solely responsible for all actions traced to the account. Sharing accounts or account passwords is prohibited. If some users need to work together in a group, they must follow the proper guidelines for work group access to files. Persons who may be liable for damage done on a shared account include the owner and any other individual who has access to the account.

- **Access to Information**
  - Unauthorized access to information contained in a user's home directory is prohibited, even if the files are readable and/or writable. When in doubt, don't read, copy, or change other users' files.
  - Any attempt to gain access or to use an email account other than by the owner will be considered a violation of network policy. Such attempts include, but are not limited to, gaining access to a user's email account while the user is away from a workstation or efforts to determine another user's password by closely watching a login.

- **Receipt and distribution of copyrighted material**
  Use of any network services, including email, for the unlawful receipt, distribution, or use of copyrighted software or material is prohibited.

- **Personal and Pecuniary Use of Resources**
  Excessive use of any District ~~any~~ network resources, including email, for personal purposes is prohibited.

- **Licensing and Copyright Infringement**
  Most software packages and applications are licensed and/or copyrighted. Most licenses and copyright agreements specifically prohibit copying or unauthorized use of the software or data.

- **Electronic Mail and Communications**
  Electronic mail (e-mail) is the primary communications tool used by network users. E-mail should not be used to transfer confidential personal information, unless the

circumstances indicate the transmission is encrypted and the sender and recipient are observing the standard of care required for the communication of confidential information by email.

- **Electronic mail privacy**
  The e-mail system is intended for official District business. E-mail messages sent or received using District communications equipment are the property of the District. Do NOT attempt to read, copy, or otherwise disturb another user's e-mail. The District reserves the right to inspect an individual's mail and/or account.

- **Controversial electronic mail/postings**
  Electronic mail is usually delivered directly from the sender to the receiver without extensive filtering. Care should be taken to keep all e-mail communications professional in nature and devoid of inappropriate language or content. Sending electronic mail messages that are determined to be obscene, abusive, hostile, harassing or otherwise offensive is considered an abuse of network privileges.

- **Forging**
  Any attempt to forge an e-mail message will be considered an abuse of network privileges and will be cause for discipline, up to and including discharge. If a user receives e-mail that could have been forged, it is in the best interests of all parties involved to confirm the e-mail with the supposed sender via personal contact. If it is determined that the e-mail is a forgery, contact the IT Help Desk. A complete copy of the message should be saved for further investigation.

- **Violation of Remote Site Policy**
  Users of remote sites or remote site services are bound by the rules and polices outlined in this document.

- **Malware**
  Anyone knowingly attempting to proliferate, create, modify, or transmit worms, ransomware, viruses, or other malware of any size, shape, or form will be terminated immediately and remanded for criminal prosecution.

- **File Transfer Protocol (FTP)**
  Using FTP to transfer files to or from remote sites that violate the policies of the remote site is prohibited and will be cause for discipline, up to and including discharge. In particular, transferring files which contain material offensive to either site, contain information to be used for personal financial interests of any party, or contain monetary or sexual solicitations is prohibited.

G. Training

All employees are required to take monthly and annual cybersecurity training. Further, the IT division will occasionally send phishing email assessments to users to make sure email users are trained appropriately.

H. Retention

The District adheres to a two-year email retention policy. In March of every year, the IT division will purge all mailboxes of messages greater than two years old after an Authorization of Disposal certificate has been received from the State of Illinois. All email received that needs to be retained as a part of the District's Document Retention Policy must be removed from email and stored elsewhere on the District data network.

~~G.~~I. Monitoring

~~Lake County Forest Preserves~~The District reserves the right (with or without cause) to monitor, access, and disclose all data created, sent, received, processed, or stored on District systems to ensure compliance with District policies, as well as federal, state, and local regulations.