SCOPE

This guideline applies to all South Metro Fire Department personnel.

DATA PRACTICES ADVISORY

During the course of employment, the South Metro Fire Department will require employees to provide data that is classified by State law as either private or confidential.

Private data is information that generally cannot be given to the public but can be given to the subject of the data. Confidential data is information that generally cannot be given to the public or the subject of the data.

The Department requests this information for various reasons pertaining to employment with the Department. The information provided may be used to process pay and benefits, evaluate performance, determine pay increases, evaluate suitability for an employee's position or other positions, determine whether disciplinary action will be imposed and other personnel actions which involve review of the employee's current and past performance.

Employees who provide false, incomplete, or misleading information may be subject to discipline, up to and including the possibility of dismissal.

Employees may not be required to provide the information requested. However, the Department may choose to require the information at any time. If required, employees will be provided with another advisory explaining that the information is required and the consequences of refusal.

Other persons or entities, if authorized by law, may receive the requested information. Depending on the data requested, these persons or entities may be: employees and/or officials of the Department who have a need to know the information in the course of their duties and responsibilities; the person who is the subject of private data about him or herself; persons who have permission from the subject of the data; insurance companies providing group benefits, worker's compensation administrative services, pre-employment, return to work and fitness for duty medical exams or drug and alcohol testing services for the Department; a public pension program; the Minnesota Department of Economic Security in a claim for or appeal for re-employment benefits; individuals who have obtained a court order for the information; and/or participants in any litigation, mediation, veteran's preference hearing, grievance arbitration, or other administrative proceeding which results from actions taken.

If litigation arises, the information may be provided in documents filed with the court, which are available to any member of the public. If it is reasonably necessary to discuss this information at a Department Board of Directors meeting, it will be available to members of the public.

To the extent that some or all of the information is part of the basis for a final decision on disciplinary action, that information will become available to any member of the public.

TYPES OF DATA

Public Data: Data about a person that must be shown to the person, if he/she wishes and that is available to other people.

Private Data: Data about a person that must be shown to the person upon request, but are not available to others without his/her permission or as otherwise specifically authorized by law.

Personnel Data: Data on individuals collected because the individual is or was an employee or an applicant for employment, performs service on a voluntary basis, acts as an independent contractor with the Department or is a member of an advisory board, committee or commission.

Summary Data: Data about a person used to develop statistics or reports are considered public information, but they do not identify the person in any way.

PUBLIC PERSONNEL DATA

Except for certain employees (i.e. undercover law enforcement personnel) the following personnel data is public:

1. name
2. gross salary
3. salary range
4. gross pension
5. contract fee
6. benefits
7. expense reimbursements
8. job title
9. job description
10. education and training background
11. previous work experience
12. dates of employment (first and last)
13. status of complaints or charges against employees
14. outcome of complaints-disciplinary action
15. work location
16. work telephone number
17. badge number
18. city and county of residence

Personnel Data on Applicants for Employment:

The following personnel data are considered public data:

1. veteran status
2. test scores
3. rank and eligibility
4. job history
5. education and training
6. work availability
7. name considered private data except when certified as eligible for an appointment to a vacancy and considered as one of the "finalists."

PRIVATE PERSONNEL DATA

The following personnel data and information are considered private data on individuals and are not accessible to the public but this data is accessible to the subject employee, the employee's authorized representative, the immediate supervisor and department head, and other Department staff persons or officials who have a legitimate need to view/know such data as determined by the Fire Chief or other persons authorized by the Fire Chief.

1. Social Security number
2. age, gender
3. marital and family status
4. employee home address and telephone numbers
5. criminal records
6. race and ethnic data

7. insurance status
8. references
9. college transcripts (except for name of institution, degree granted, and date)
10. reference check data
11. medical records when part of personnel data
12. psychological evaluations
13. worker's compensation reports
14. physical limitations related to the job
15. sick leave forms - doctor's reports
16. data collected from disciplinary proceedings prior to a hearing
17. opinion questionnaire response by potential employee
18. names of applicants for employment until certified as eligible for appointment to a vacancy.
19. employee assistance programs and exit interview responses

No employee may disclose the home address, telephone number, or personal information about another employee to any third party without prior consent of the affected employee, as per Section on "Informed Consent."

Employment selection instruments and/or answer keys to such instruments are protected non-public data, except pursuant to a valid court order.

ACCESS TO DATA

Public Data:

Access shall be provided to any person, without regard to the nature of the person's interest. Access must be approved by the Fire Chief or other persons authorized by the Fire Chief. Access must be provided within a reasonable time. Interpretation shall be provided if requested. A fee may be charged, as allowed by law, reflecting time to collect or retrieve the information, paper costs, mailing costs, duplicating costs, etc.

Private Data:

Access is available to the following only:

1. The subject of the data.
2. Individuals whose work assignments with the Department reasonably require access.
3. Entities and agencies determined by the Fire Chief or his/her designee to be authorized by State Statute or Federal Law to gain access to that specific data.
4. Entities or individuals given access by the express written direction of the subject.

The Fire Chief or authorized designee shall assure that access is provided only to the parties listed above. The identity and authority of an individual who seeks to gain access to private data must be confirmed. The time that access is available is limited to the normal working hours of the Department offices. No fees shall be charged in the instances where the data subject only wishes to view private data. Fees may be charged for providing copies.

GENERAL CONTENTS OF PERSONNEL FILES

The following information shall routinely be included in an employee's personnel file:

1. data collected for administrative purposes such as job applications, resumes, confirmation letters, change of address forms, training or education records, veteran's certification, etc. (Documents containing medical information are retained in a separate medical file.)

2. documentation of personnel actions or activities such as salary changes, job classifications, performance reviews, termination notices, disciplinary actions.

3. official written correspondence to or from an employee (subject to determination by the Fire Chief/HR Director as to appropriateness).

4. documentation of employment status and benefit status, the latter only if it does not contain any medical information. Appropriate medical information will be retained separately in an employee medical file.

Employees will not be specifically notified each time such data are routinely entered into their file, except that employees shall be made aware of data entered into their file that relates to discipline or may have adverse impact on them. Employees may request to view and receive copies of information in their file as per Section on "Access to Data."

Personnel files will be maintained by the Fire Chief or with assistance from appropriate Administration support staff. Any documents added or removed from the files must be approved by the Fire Chief. The Fire Chief may delegate the authority to add routine and non-controversial documents (such as job applications, employment confirmation letters, status change forms, etc.) to other staff as appropriate. Such staff shall be trained on this policy.

TAPE RECORDING POLICY

In order to protect the regulation and dissemination of confidential, private, and non-public data as defined in the Minnesota Government Data Practices Act; promote harmony in the work place, diminish the impediment of each employee's ability to perform his or her duties, and promote an environment with a free-flow exchange of ideas: inter-staff communications shall not be tape-recorded in any form unless all parties to the communication consent or the meeting being recorded is a meeting of the Department Board of Directors.

In the event a tape recording is created, the Fire Chief or other persons authorized by the Fire Chief shall immediately receive, keep, and maintain the tape recording and shall regulate the dissemination of the information in accordance with the Minnesota Government Data Practices Act.

INFORMED CONSENT

Private data on individuals may be used by and given to any individual or persons by the Fire Chief or other bonafide representative of the Department, if the individual subject or subjects of the data have given their informed consent. All informed consents:

1. Shall be in writing and stated in plain language.
2 Shall be signed and dated.
3. Shall specifically designate the particular persons or agencies the data subject has authorized to disclose information about him or her.
4. Shall specifically state the nature of the information authorized to be disclosed.
5. Shall specifically state the persons or entities authorized to receive the disclosed information.
6. Shall specifically list an expiration date not to exceed one year.
7. Shall specifically state the purpose for which the information may be used by the parties named above.

If the Fire Chief or other persons authorized by the Fire Chief makes reasonable efforts to obtain the informed consent of a data subject and if those efforts are not acknowledged in any way, the Fire Chief or other persons authorized by the Fire Chief shall interpret the silence of the data subject as the giving of implied consent to the new or different purpose or use of the data.

"Reasonable efforts" are defined as:

1. Depositing in the U.S. Mail, postage pre-paid, and directed to the last known address of the data subject, at least two (2) communications requesting informed consent.

2. Waiting for a period of not less than sixty (60) days for a response to the second request.

SECURITY OF PERSONNEL DATA

The South Metro Fire Department authorizes the Fire Chief and individuals responsible for providing support to the Department's human resource function to maintain custody over all personnel records. The final authority over personnel records is the Fire Chief, and as such, retains overall authority to add or remove items from personnel and related employee files.
All records containing non-public personnel data shall remain in one or more locked filing cabinets, or other locked storage facility, with keys strictly limited to those designated to maintain custody. Others authorized to review personnel records, such as the subject of the data, or as described above under "Access to Data, Private Data," shall be required to view the contents of such files in the presence of authorized staff. No access to keys securing the information may be provided to anyone not authorized to maintain custody. All keys must be properly secured at all times to prevent improper access to files.

Personnel files shall not be removed from Fire Chief Office. Copies of file contents may be removed from Department offices only by individuals authorized to have access to those records, consistent with the Minnesota Government Data Practices Act and this policy. Unauthorized release of private and/or confidential personnel data shall be subject to immediate discipline, up to and including termination.

SUPERVISORY FILES

Information about employees maintained by supervisors is considered personnel data under State Statute and must be maintained in a locked area by supervisors. Supervisors may not maintain medical information on employees.

Types of data maintained by supervisors shall be limited to that authorized by the Fire Chief, consistent with law and policy. Examples of personnel data supervisors are authorized to maintain include:

1. vacation leave slips and other time-related records,
2. notes from supervisory coaching and counseling sessions,
3. notes on performance concerns or work rules discussed with employees, (to be removed after entry in annual performance evaluation)
4. notes on employee accomplishments, (to be removed after entry in annual performance evaluation)
5. copies of disciplinary and performance-related correspondence. (Copies of disciplinary letters may be maintained in supervisory files after ensuring a copy has been confidentially forwarded for inclusion in the employee's official personnel file.)

All original Department applications and related hiring documentation, performance evaluations, reference information, doctor's slips and other medical information about employees must be submitted to the Fire Chief. The Fire Chief will determine which documents will be maintained in Department personnel files, consistent with this policy. The personnel files maintained by the Fire Chief and authorized Administration staff are considered the official Department Personnel files.