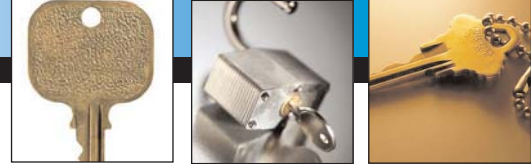




OPS Human Resources **Privacy & Security** **Guidelines**

**Centre for Leadership and
Human Resource Management**

July 2005



INTRODUCTION

Employment related information is governed by many statutes including the:

Public Service Act;
Ontario Human Rights Code;
Occupational Health and Safety Act;
Public Sector Salary Disclosure Act; and
Personal Health Information Protection Act (PHIPA).

This policy is informed by those statutes as well as by other policies that may be in place.

Employee-Related Information

The phrase "employee-related information" covers both employee-specific information as well as more general human resources information.

a) Employee-specific information refers to files such as corporate employee files, competition files or health-related files, or to information in files related to an employee including employment history, resume, references, actual salary and benefits, performance appraisals, attendance data, rewards and recognition information, WSIB, medical and accommodation information, and grievances, discipline, investigations and security information.

b) Personal information refers to recorded information about an identifiable individual.

c) General human resources information includes information such as HR planning, labour relations strategies, job evaluation and classification determinations and workforce and succession planning.

The *Freedom of Information and Protection of Privacy Act* (FIPPA) does not apply to employment-related information except:

1. an agreement between the employer and a trade union;
2. a settlement agreement between the employer and one or more employees;
3. an agreement between the employer and one or more employees; and
4. an expense account submitted by an employee to the employer.

PURPOSE

This guideline outlines best practices for privacy protection of employment-related information and access to general human resources information. It also outlines the main types of employee-related information gathered within the OPS and provides direction for the collection, use, and disclosure of personal and other employment information and access to it.

This guideline has been prepared with a view to balancing the rights of employees to privacy and access with the rights and needs of the OPS to collect and maintain information necessary for the effective management of its workforce.

Standards on the use of information technology equipment in the workplace are already in place that address privacy and access from an information technology perspective. The standards can be found on the Access and Privacy Office website under *Electronic Service Delivery Privacy Standard*.

PRINCIPLES GOVERNING EMPLOYEE-RELATED INFORMATION

The following principles have been developed as a guide to the handling of employee-related information and form a benchmark for Ministries to use in developing processes and procedures tailored to meet their individual operations and needs.

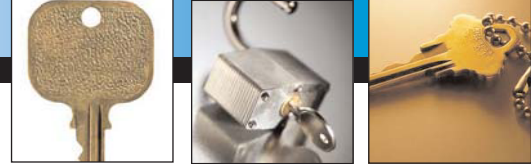
1. Collection

Collection involves obtaining information on an identifiable employee. Information on an employee is collected only when it is necessary and when the employee has expressly consented in writing or when there is implied consent.

The collection of employee information for the purposes of pay and benefits administration is an example of implied consent, while a signed consent form to contact references constitutes written consent.

2. Use

The nature and extent of personal information that is compiled and shared should be limited to what is required for the task at hand and should only be shared and discussed on a "need-to-know" basis within the ministry, with anyone in another ministries, or with anyone outside the OPS.



There are many situations when advice can be sought, or a discussion can take place, without disclosing the identity of the employee involved. A standard best practice is to keep the employee's identity anonymous in such discussions, unless it is directly relevant and needed for the purpose at hand.

3. Disclosure

Personal information should only be disclosed when it is necessary for the duties to be performed and limited to what is needed to carry out the task. Disclosure should also be consistent with the purposes for which the information was collected and, in cases where a consultant is used, only when appropriate steps have been taken for disclosure to a third party (See page 4, *Access by Consultants*.)

There may be unique instances when obtaining consent is impractical. For example, in an emergency situation such as when an employee is injured or ill, it may be necessary to disclose personal information about an employee in order to notify next of kin or to call an emergency contact of the employee's for assistance. While it may be appropriate to disclose this information without consent, care should be taken to ensure that only the minimal necessary information is disclosed.

4. Security

Procedures must be in place to ensure that personal information is kept secure and confidential. Ministries are responsible for:

- a) Developing and implementing procedures to safeguard the security of employee-related information held in files. This includes ensuring that personal information is properly locked and stored.
- b) Restricting access to a "need-to-know" basis and determining appropriate access levels, protocols and audit trails.
- c) Safeguarding security when transferring material containing personal information within the Ministry and from one Ministry to another.

5. Access

Principles of access relate to both employee access to their own personal information, and access by others to information about an employee.

a) Full Employee Access to Information

Employees should be provided with access to information pertaining to them that is contained in their corporate files and to files containing their health-related information.

b) Limited or No Employee Access to Information

Some files have certain restrictions. For example, employees can access information about their own results from a competition file, but not information on the results of others. Other files, such as those dealing with labour relations, or solicitor-client privileged information, should not be provided to the individuals about whom they relate unless there is specific authority.

Access By Others to Information

Access to employee-related information should be limited to individuals addressing a particular issue on a "need to know" basis.

Access by Consultants

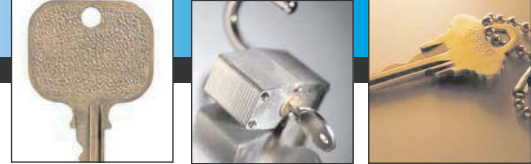
The standards for privacy and security established in these Guidelines apply to any consultant who is hired and requires access to personal information. Steps must be taken to ensure that legally binding language is used in consulting agreements to ensure that consultants are bound to handle personal information in accordance with the Guidelines, that they have been briefed on these requirements prior to commencing work, and that a follow-up review is conducted to ensure consultants complied.

6. File Transfer

The Crown, rather than an individual Ministry, is considered to be the employer when dealing with employee-related information. As a result, personal information such as an employee's corporate file can be transferred from one Ministry to another to accompany a transferring employee with the appropriate security safeguards in place.

7. Retention

Ministries must take steps to ensure that information is retained only for the period authorized by the Ministry retention schedules and the Records and Information Management Directive, and that information is disposed of in a way that ensures that the identity of the individual is not accessible after its disposal.



TYPES OF RECORDS

CORPORATE EMPLOYEE FILES

An employee corporate file is compilation of key information and actions relating to an employee throughout the course of his/her employment with the OPS.

Contents

A corporate file normally includes the following documents:

Resume; signed hiring offer letter; oaths, pay and benefits documentation; WEAR forms; emergency contact information; signed copies of finalized performance appraisals; signed copies of any acting, secondment, transfer or assignment agreements; signed acceptance of promotional offer letters; copies of any awards or settlements; any reward, recognition or commendation letters; key training and development and career planning information; and any disciplinary documentation.

Documents that Identify More Than One Employee

From time to time, a document to be placed on an employee's corporate file, such as a commendation, award or settlement, identifies more than one employee. In such circumstances, the names of other employees should be blocked out to preserve their privacy, since only information pertaining directly to the specific employee should be placed in his/her corporate file.

Accuracy and Completeness

As a record of key hiring and employment-related activities and actions, Ministries should establish procedures to ensure that all relevant documents are forwarded to, and filed in, the employee's corporate file. Placing the employee's WIN number on all documentation sent to the corporate file is one way of minimizing confusion or filing errors.

Ministries are also responsible for ensuring that corporate files are up-to-date and that information to be removed from an employee's corporate file, such as disciplinary documentation, is done so after the period specified for its retention in the relevant collective agreement.

Employee Access to His or Her Own Corporate File

Ministries should establish procedures for making the corporate file available to employees wishing to view their own personal information contained in the corporate file. A file review should be conducted prior to granting access to ensure that no inappropriate information (such as information identifying another employee or third party or privileged labour relations or security-related material) has inadvertently been placed in the file. While the employee may view the file, care should be taken to ensure that documentation is not removed or altered.

Employee Changes or Disagreement with File Content

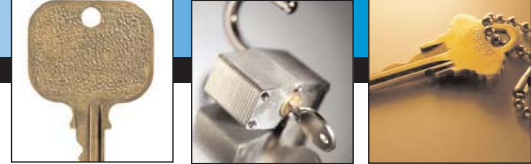
In the event an employee identifies errors or incomplete personal factual information, the employee can submit a request for correction. Factual errors should be corrected. In the event that an employee disagrees with a document or opinion in his/her corporate file that is not of a factual nature, the employee is allowed to prepare a "statement of disagreement" document for submission to HR staff for inclusion in his/her corporate file.

Access to Corporate Files by Others

Access to employee corporate files should be provided on a "need-to-know" basis. Ministries should establish controls for individuals with designated routine access and for authorizing limited access. This includes protocols for access by individuals in circumstances an employee would reasonably expect their information to be accessed and used. For example, it would be reasonable to expect access for the purposes of pay and benefits administration and in the course of making a promotional decision.

Consent to Access Corporate File by External Entity

An employee's written consent is required before providing access to his/her corporate file by an external entity, such as his or her lawyer. The consent form should be filed in the employee's corporate file and a record of the access maintained.



Archiving Corporate Files

Employee corporate files are archived in accordance with Ministry records retention schedules and as provided in the Records Information Management Directive. By providing adequate notice, they can be retrieved on a "need-to-know" basis by HR personnel.

Local Personnel Files

In some instances, a local personnel file may be maintained in addition to a corporate file, particularly where the corporate file is kept off-site. Since the information in the local file mirrors the corporate file, the same access and privacy provisions apply.

A manager's working copy of documents, notes and other information compiled to assist in carrying out managerial responsibilities should be kept independent of a local file.

Files for Employees Transferred on a Temporary Basis to Another Ministry

From time to time, employees may be assigned for a specified period to a Ministry other than their home one (i.e. for acting periods, secondments, or temporary assignments). As information relevant to the employee may be acquired during the temporary period that should eventually find its way to the employee's corporate or health-related file, Ministries should establish protocols for addressing the collection and storage of this information. One option would be to create a temporary file and eventually transfer relevant information to the employee's corporate or appropriate health-related file at the end of the temporary period, or for requesting the transfer of the file(s) for the duration of the temporary period.

COMPETITION FILES

Contents

The competition file should contain all final documents reflecting every aspect and phase of the competition process, including the JIP; resumes; screening and assessment tools and results; interview schedule, questions and rating guide; individual candidate assessments, reference information and consent forms; summary of ranking; and job offer results.

Notice of Collection of Personal Information

Any requirement for the collection of personal information, such as medical, security or credit, as part of the screening or selection process should be communicated in the job ad so that individuals can make an informed decision about applying. Written consent for such checks must be provided before they can be conducted. While the final outcome of such checks (i.e. medically fit or not fit, passed or did not pass a credit check) needs to be filed to substantiate the competition results, other documentation regarding the check itself should be filed separately in security, medical or other files as appropriate.

Conducting Reference Checks

Candidates must provide written consent for references to be contacted. Information in a reference check should focus on obtaining relevant information necessary for an assessment of the candidate in relation to the position being filled.

Providing Reference Checks

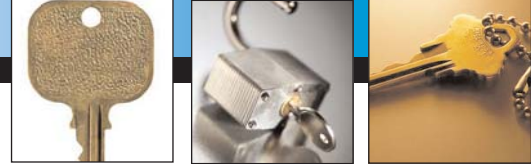
Providing a reference on behalf of an employee should be limited to performance information relevant to the position for which the employee has applied. Confirmation regarding the confidentiality of information provided should be sought before proceeding. Health-related information or violation-of-law information should only be obtained when specific consent for the collection of this information has been obtained and verified.

Notice of Retention in Inventory

Candidates should be advised if information pertinent to them arising out of a particular competition will be retained in an inventory for potential future consideration. This could take the form of information provided in a job ad or in subsequent communications with the candidate.

Candidate Access to Job Competition Information

Once a competition has been finalized, access to information and feedback about a candidate's own performance throughout the process can be provided. Access to the competition file or copies of documents other than what is generally made available to candidates (such as job descriptions or organizational information), should not, however, be provided to ensure the confidentiality of other candidates and to ensure the integrity and confidentiality of the screening and selection tools used.



Competition File Retention

The hiring manager for the competition is responsible for the file security and for ensuring that it is retained and archived in a keeping with the OPS retention schedule.

Access to the Competition File

As the person responsible for the retention of the competition file, the hiring manager is also responsible for providing access to the competition file on a "need-to-know" basis. This could be, for example, to a selection panel member or HR Consultant involved in the competition process in order to debrief a candidate or to respond to an enquiry or issue involving the process.

The hiring manager may also receive requests, from time to time, to access the competition file by other managers seeking to utilize some of the selection tools used in the competition. In adherence to the principles of providing only information necessary to the task at hand, only the relevant selection tools requested, rather than the entire file or any document referencing an individual, should be made available to preserve the confidentiality of candidates.

HEALTH-RELATED INFORMATION AND FILES

Types of Health-Related Information

In the course of employment, health-related issues may arise that result in or necessitate the collection of health-related information that falls into one of the following categories:

- Work-related injury (WSIB)
- General health-related information (absences, illnesses, LTIP)
- Accommodation

Maintaining Separate Health-Related Files

The sensitive nature of this information warrants extremely limited access to it on a "need-to-know" basis and it should not, therefore, be contained within a corporate file. Maintaining separate files for WSIB, general health information, and accommodation safeguards the confidentiality of the information and significantly reduces access to only the small number of individuals involved in the resolution of a specific issue. Separating and centralizing this information will result in more complete information being available in one source when an issue does arise.

Nature of Medical Information Retained in Files

Apart from the WSIB file, medical information in other files should be limited to prognosis, not diagnosis, and any work restrictions, accommodation, or return-to-work needs of an employee. It should also include the actions taken to address the health-related needs.

Consent for Health-Related Information

In the event that additional information is required from a medical practitioner, the employee must sign a consent form before such information can be requested.

Employee Access to Health-Related Information

These files contain information an employee either already knows, has consented to, has access to through another mechanism, or has been compiled on his or her behalf, and should be made available upon request.

DISCIPLINE, LABOUR RELATIONS, INVESTIGATIONS (INCLUDING WDHP)

Exchange of Information

Exchange of information, correspondence and other documents relating to an employee involving labour relations, discipline, or during the course of an investigation, should be limited to those who need to be involved in the resolution of the specific issue, whether inside the organization or externally.

Consent to Disclose Information

Employee consent is not required to disclose personal information to a bargaining agent, when providing personal information to a law enforcement agency conducting an investigation, for investigations conducted by the Worker's Safety and Insurance Board, Employment Standards, or to a court or an administrative tribunal, in accordance with the rules of the court or tribunal. Consent is also not required for the purposes of complying with a statute, such as investigations under the Ontario Human Rights Code or for an internal investigation or audit. However, advice from counsel or an internal specialist should be sought before providing information of this type to ensure that it is provided appropriately.

Generalized public monitoring where the health and safety of employees may be at issue, such as at public service counters, may warrant a public notice stating that operational surveillance is being carried out.

No Access to Files

Employees do not have access to disciplinary, labour relations or investigation files. Seek legal advice when an issue of access to such files by an employee arises.

REPORTING PRIVACY BREACHES

A privacy breach occurs when personal information is collected, used, disclosed or retained in ways that are not in accordance with the principles established in these Guidelines. Among the most common breaches of personal privacy is the inappropriate disclosure of personal information. For example, personal information may be lost (an employee taking personal information home loses his/her briefcase on public transit), stolen (a computer containing payroll data is stolen from an office) or inadvertently disclosed through human error (a letter informing an applicant about the results of a competition is inadvertently mailed to the wrong individual).

An employee involved in a privacy breach, or who becomes aware of a breach, must immediately notify his or her direct report or another manager and take steps to control it. The FOI Coordinator or Legal Counsel must be contacted to ensure that appropriate actions are taken to address the breach. The employee must be prepared to provide as much detail about the breach as possible. The sooner a breach is identified, the quicker appropriate actions can be taken to contain and manage it.

OTHER HUMAN RESOURCES INFORMATION

More General Human Resources Information

The broad range of human resources information such as workforce planning, job evaluation, and labour relations strategies is not considered to be employee-specific or personal information. The nature and extent that it is made available to employees is at management's discretion.

It is important to note for clarity that work produced by named employees as part of their job responsibilities, such as a policy paper developed by a particular employee, does not constitute the personal information of the named employee.

