DOCUMENT RESUME

ED 429 576 IR 019 537

| | |
|---|---|
| AUTHOR | Gillis, R. Peter; Whitemarsh, Judith |
| TITLE | FOIPP and Technology: Best Practices for Alberta School Jurisdictions. |
| INSTITUTION | Alberta Dept. of Education, Edmonton. |
| ISBN | ISBN-0-7785-0341-0 |
| PUB DATE | 1999-02-00 |
| NOTE | 107p.; A publication of the School Technology Task Group. For related document, see IR 019 538. |
| AVAILABLE FROM | Learning Resources Distributing Centre, 12360-142 St., Edmonton, Alberta, Canada T5L 4X9; Tel: 780-427-5775; Fax: 780-422-9750; Web site: http://ednet.edc.gov.ab.ca/technology/ |
| PUB TYPE | Guides - Non-Classroom (055) -- Reports - Descriptive (141) |
| EDRS PRICE | MF01/PC05 Plus Postage. |
| DESCRIPTORS | *Access to Information; Check Lists; Computer Security; *Computer Uses in Education; Educational Administration; Educational Practices; Educational Technology; Elementary Secondary Education; Foreign Countries; *Freedom of Information; Information Management; *Information Policy; Information Systems; Information Technology; Legislation; *Privacy; *School Districts |
| IDENTIFIERS | Alberta; Technology Implementation |

ABSTRACT

This study provides suggestions and best practices for superintendents, Freedom of Information and Protection of Privacy (FOIPP) coordinators and school information technologists in dealing with the impact of Alberta's FOIPP Act on the application of information technologies within their organizations. The study explores the relationship between the requirements of the legislation and the ongoing application of technology within school organizations, as it relates to accessing information, protecting individual privacy, and managing electronic information. The study is divided into six parts: (1) FOIPP overview and checklist for senior managers; (2) introduction, covering the scope of the FOIPP Act and definitions; (3) accessing general information, including policy principles for information access; (4) accessing personal information; (5) protecting personal privacy, including privacy requirements, implementing privacy protection for information systems, planning new and modified personal information systems, privacy impact assessment, security of personal information, and contracting; and (6) FOIPP and information management, including managing electronic records, security, and e-mail. Appendices include strategies for school jurisdictions, basic questions for school jurisdictions, and related Alberta Education resources. (AEF)

# FOIPP AND TECHNOLOGY

## Best Practices
## For Alberta School Jurisdictions

February, 1999

Information Sharing Forum
TECHNOLOGY

Alberta
EDUCATION

ALBERTA EDUCATION CATALOGUING IN PUBLICATION DATA

Alberta. Alberta Education.
FOIPP and technology : best practices for Alberta school jurisdictions.

Available on the Internet: http://ednet.edc.gov.ab.ca/technology/
ISBN 0-7785-0341-0

1. Freedom of information - Alberta. 2. Privacy, Rights of - Alberta.
I. Title.

KEA505.62.A333 1998 342.0853

Additional copies are available through:

Learning Resources Distributing Centre
12360–142 Street
Edmonton, Alberta, Canada T5L 4X9
Telephone: 780–427–5775
Facsimile: 780–422–9750

For more information, contact:

Bonnie Brooks
School Technology Task Group
Alberta Education
11160 Jasper Avenue
Edmonton, Alberta, Canada T5K 0L2
Telephone: 780-427-9001
Facsimile: 780-415-1091

To be connected toll free outside Edmonton, dial 310-0000.

The primary intended audience for this framework is:

| | |
|---|---|
| *Administrators* | ✓ |
| *Counsellors* | |
| *FOIPP Co-ordinators* | ✓ |
| *General Audience* | |
| *Information Technologists* | ✓ |
| *Parents* | |
| *Students* | |
| *Teachers* | ✓ |

# PREFACE

This study provides suggestions and best practices for superintendents, FOIPP co-ordinators and school information technologists in dealing with the impact of the *Freedom of Information and Protection of Privacy (FOIPP) Act* on the application of information technologies within their organizations. This **is not** a general guide to interpreting and implementing the *FOIPP Act* in school jurisdictions. Rather, the study explores the relationship between the requirements of that legislation and the ongoing application of technology within school organizations, as it relates to accessing information, protecting individual privacy and managing electronic information. The study places an emphasis on the development of new applications of information technology but many of the same principles and practices can be used to review existing information systems. As well, the overwhelming focus is on automated electronic systems but, again, many of the same approaches can be applied to paper, microfilms and audio and visual records that are not in electronic format.

The study consists of two distinct sections:

1. Part 1: A management overview and checklist for use by superintendents and other senior administrators. This section summarizes various strategies to integrate FOIPP requirements into the application of technology and raises basic questions that should inform implementation of this aspect of the *FOIPP Act*.
2. Parts 2–6: A more detailed specialist document. This section will help FOIPP co-ordinators and those responsible for developing information technology applications within school jurisdictions to deal with the various access and privacy provisions of the *FOIPP Act* as they impact on the application of information technologies. Part 5 includes a management tool for undertaking privacy impact assessments for new information systems. The strategies and basic questions included in Part 1 are woven throughout the appropriate parts of the document.

Broader interpretation and practices relating to the *FOIPP Act* can be found in the *Freedom of Information and Protection of Privacy Policy Guide*. The *Guide* is produced by the Information Management and Privacy Branch of Alberta Labour, which acts as the representative of the Responsible Minister (Minister of Labour) in providing advice concerning the province-wide administration of the *FOIPP Act*.

If there is a need for additional clarification, advice may be sought from the Office of the Information and Privacy Commissioner at:

Office of the Information and Privacy Commissioner
410, 9925–109 Street
Edmonton, Alberta, Canada T5K 2J8
Telephone: 780–422–6860
Facsimile: 780–422–5682
E-mail: ipcab@planet.eon.net

# ACKNOWLEDGEMENTS

Alberta Education wishes to acknowledge the contributions of the following individuals.

## PROJECT DIRECTOR

| | |
|---|---|
| Dale Erickson | Alberta School Boards Association |

## AUTHORS

| | |
|---|---|
| R. Peter Gillis | RPG Information Services Inc. |
| Judith Whitemarsh | RPG Information Services Inc. |

## SCHOOL TECHNOLOGY ADVISORY COUNCIL MEMBERS DURING DEVELOPMENT

| | |
|---|---|
| John Travers (Chair) | Alberta Education |
| Peter Balding | Black Gold Regional Division No. 18 |
| Marika Bourque | Calgary School District No. 19 |
| Bonnie Brooks | Alberta Education |
| George Buck | Universities Co-ordinating Council |
| David Burch | Alberta Home and School Councils' Association |
| Edna Dach | Elk Island Public Schools Regional Division No. 14 |
| Jack Dale | Calgary School District No. 19 |
| Peter Darby | Chinook's Edge School Division No. 73 |
| John Darroch | Palliser Regional Division No. 26<br>College of Alberta School Superintendents |
| Dale Erickson | Alberta School Boards' Association |
| Chris Farthing | Edmonton Catholic Regional Division No. 40 |
| Toni Hafso | Alberta Education |
| Gary Heck | Lethbridge School District No. 51 |
| Harry Henshaw | Alberta Education |
| Robert Hogg | St. Albert Protestant Separate School District No. 6<br>The Alberta Teachers' Association |
| Maurice Hollingsworth | Palliser Regional Division No. 26 |
| Judi Hunter | Calgary School District No. 19 |
| Glen Johnson | Edmonton School District No. 7 |
| Doug Knight | Alberta Education |
| Catherine Kullman | TELUS Learning Connection |
| Norma Nocente | Universities Co-ordinating Council |
| John Percevault | Grande Yellowhead Regional Division No. 35 |
| Archie Pick | Alberta Chamber of Resources |
| Doug Pudwell | Medicine Hat School Division No. 76<br>Association of School Business Officials of Alberta |
| Randy Rudd | Pembina Hills Regional Division No. 7<br>College of Alberta School Superintendents |
| Ralph Schienbein | Elk Island Public Schools Regional Division No. 14 |
| Jacqueline Skytt | The Alberta Teachers' Association |
| Ron Sohnle | Alberta Education |
| Gary Spence | Wolf Creek School Division No. 72 |
| Lonnie Springer | Calgary Roman Catholic Separate School District No. 1 |
| Mary Stephenson | Alberta Chamber of Commerce |
| Barbara Stevenson | Calgary School District No. 19<br>The Alberta Teachers' Association |

| | |
|---|---|
| Paul Stevenson | Horizon School Division No. 67 |
| Arwin van Voorthuizen | Alberta College of Art<br>Council of Presidents of Public Colleges and Technical Institutes of Alberta |

## RESOURCE PERSONNEL

| | |
|---|---|
| John Hogarth | ConsultNet |
| Peter Wright | University of Alberta |

# TABLE OF CONTENTS

# CHARTS

# PART 1: OVERVIEW AND CHECKLIST FOR SENIOR MANAGERS

## OVERVIEW

The *Freedom of Information and Protection of Privacy (FOIPP) Act* came into effect for school jurisdictions on September 1, 1998. The provisions of the legislation have a profound impact on how schools and school jurisdictions will apply and use information technology in the future, both in regard to accessing information and protecting individual privacy. This study is intended to help school administrators, FOIPP personnel and those involved in developing and implementing electronic systems to better understand the *FOIPP Act* as it relates to the application of information technologies and to aid them in devising strategies and approaches to effectively deal with its requirements.

The study is oriented toward technology perspectives, but a good portion of the discussion and approaches are applicable to wider FOIPP matters.

## SCOPE OF THE *FOIPP ACT*

The *FOIPP Act* expresses five basic purposes that can affect the application and use of information technology in school organizations. These are as follows:

- a right of access to records;
- a right of access by individuals to information about themselves;
- a right of individuals to seek correction of information about themselves when they are of the opinion there has been an error or omission;
- protection of the privacy of individuals who provide information to school organizations; and
- independent review, through the Information and Privacy Commissioner, of any decision or action taken by the school organization that relates to any duties, obligations or requirements covered by FOIPP legislation.

These purposes impact on the application of information technology in school jurisdictions in four basic domains:

- accessing of general information;
- students, parents and employees accessing personal information about themselves;
- protection of privacy in the development and management of electronic information systems that deal with personal information; and
- the overall management and protection of the information resources of school jurisdictions.

Each of these domains is discussed below and major issues addressed. Useful questions for officials, employees and teachers when dealing with FOIPP and technology applications are provided for each domain. These are designed to act as signposts for strategies and approaches that can support both successful administration and management of the access and privacy legislation and innovative and effective application of information technology.

## ACCESSING GENERAL INFORMATION

FOIPP requests are both expensive and time consuming to process and are sometimes confrontational in nature. FOIPP requests should be viewed as the avenue of last resort in dealing with persons who may wish to obtain information about schools or school administration within your jurisdiction.

***Strategy***[1]

Continue and strengthen current methods of communicating with students, parents, employees and the public-at-large, and seek to expand this informal, non-FOIPP approach to providing information. Develop an information access policy that enables your organization to be proactive in providing access to information and to avoid reacting to demands for information through FOIPP requests.

Sections 83 and 84 of the *FOIPP Act* enable this approach. They provide that:

- categories of records may be established where access to the information can be provided outside the FOIPP process;
- independent fee structures may be set to cover access costs; and
- manuals, guidelines and handbooks used to administer or operate an organization are to be made available to the public.

These sections are intended to support openness, accountability and transparency within school organizations.

***Strategy***

To the extent possible and where it is practical, employ information technology to support regular disclosure of information outside the FOIPP process in order to better meet educational objectives and avoid FOIPP requests, while implementing the spirit of the *FOIPP Act* for more open, accountable and transparent administration of school jurisdictions.

There are two distinct approaches to broadening disclosure of information outside the *FOIPP Act*—routine disclosure and active dissemination.

[1] A comprehensive list of strategies referenced throughout this document is included in Appendix A.

*Routine disclosure or disclosure without a FOIPP request* occurs when access to a record can be granted without resort to a request under the *FOIPP Act*.

*Active dissemination* occurs when information or records are periodically released (without any request) under a program or release strategy. This is best used where there is a strong and constant demand for information that would be available to the public.

Excellent candidates for such types of non-FOIPP disclosures are situations where:

- disclosure is mandated by another statute or by-law and the records will be released;
- no exceptions (i.e., the *FOIPP Act* has no provision for refusing access) apply to records;
- no mandatory exceptions apply to a class of records (i.e., the *FOIPP Act* requires that access be refused) and the school jurisdiction has decided not to invoke any discretionary exceptions; or
- exceptions apply to a class of records but the sensitive information can easily be suppressed from information that then may be routinely disclosed.

The establishment of electronic information systems, including an Internet site for an organization, provide an avenue for establishing mechanisms where routine access or active dissemination may be considered. Initially the impetus may come from a variety of external sources:

- demand from parents for more accountability;
- media reports critical of school jurisdictions for concealing information and not being accountable to parents;
- complaints from taxpayers about high fees for preparing customized information reports; or
- a burgeoning number of FOIPP requests and orders from the Information and Privacy Commissioner that result in large amounts of information being released through FOIPP at considerable cost to the school jurisdiction.

***Strategy***

Use electronic media and formats, including public networks, as appropriate and within budgetary constraints, in order to make information more easily accessible and useful to students, parents and the public. Such efforts, however, should not preclude those without access to computer technologies from accessing similar information by other means; for example, publications, library sources, etc.

## PRACTICES FOR ROUTINE DISCLOSURE/ACTIVE DISSEMINATION

Routine disclosure and active dissemination (RD/AD) should become a normal part of your organization's operations and a support for improving its performance. To the extent possible, information technology should be used to accomplish this goal.

Release and dissemination can take several forms, such as:

- release of particular information whenever a student, parent or other member of the public requests it as part of the service being offered;
- use of information and document centres to provide information, including access terminals and mail and fax services for information;
- use of reference databases to answer frequently asked questions from students, parents and the public;
- publication of self-browse and self-service database services;
- distribution of databases to libraries and other public facilities or use of private sector information services to mount popular public databases; and
- use of the Internet and other public networks to distribute information.

Where a school jurisdiction is larger in size or decentralized in operation, it may be advantageous to develop a network of contacts in program and administrative areas. This may be built into a co-ordinating group, which is mandated to develop a corporate approach on routine disclosure and active dissemination and to help implement such disclosure practices.

Members of such a group should include:

- the FOIPP co-ordinator, who can assist in interpreting the *FOIPP Act*;
- interested staff and teachers with information that may well qualify for routine disclosure and active dissemination;
- a communications officer involved in information release and dissemination; and
- a representative from the information technology area who understands how the public body can use the new information networks to release and disseminate information.

Either the FOIPP co-ordinator or a special co-ordinating committee should develop a corporate information access policy.

## CREATION OF NEW INFORMATION SYSTEMS

The corporate policy on routine disclosure and active dissemination should require that the FOIPP co-ordinator be consulted when there are plans to create new information systems within the school jurisdiction. This consultation should determine whether or not any of the new information could be released outside FOIPP.

All dissemination projects involve investment of resources by school jurisdictions, and these costs have to be balanced against improved services to students, parents and the public and possible avoidance of FOIPP requests.

When considering dissemination of electronic products, public bodies should, whenever appropriate and within budgetary constraints, consider using public and local networks such as the Internet, freenets and civic networks.

### *Basic Questions*[2]

The following questions should be posed to the organization when dealing with issues over access to information.

- ❑ Does our organization currently have in its custody or under its control information that:
  - is in demand; and
  - the release of which in a proactive and informal manner would better meet the concerns of students, parents and the public for more open and accountable governance of our school, board or district?
- ❑ Could we release such information either on a routine basis or through active dissemination without compromising those mandatory interests, particularly personal privacy, which we are required to protect under the *FOIPP Act*?
- ❑ Do the current technology applications which we are undertaking or planning to undertake in the near future, including use of the Internet, adequately take into account the need for the routine disclosure or active dissemination of this type of substantive organizational records?
- ❑ Have we or are we going to automate the creation and management of our organization's manuals, handbooks or other guidelines that the *FOIPP Act* requires must be made available to the public? Have we recognized this requirement as part of the management application?
- ❑ Do we have an information access policy and an ongoing process in place to identify such sources of information and to ensure that they are made available in ways that meet our overall business objectives?
- ❑ Do we release such information in forms (electronic and paper) which meet the needs of students, parents and the public?
- ❑ To the extent that we permit public access to electronic information (for example, an Internet site), do we have adequate technical safeguards in place to ensure that no access is permitted to our electronic information systems beyond these public data sources?

[2] A comprehensive list of basic questions referenced throughout this document is included in Appendix B.

## ACCESSING PERSONAL INFORMATION

The *FOIPP Act* provides that individuals or their representatives may access personal information, subject to limited and specific exceptions. There are fewer exceptions to access that apply to situations where individuals are requesting access to information about themselves. As well, fairness dictates that such information is provided to them unless there are very strong reasons why access should be refused; for example, the information may harm the physical or mental health of the applicant.

School jurisdictions may be able to identify categories of records containing personal information that may be made available routinely **only to the individual** that the information is about. This may be done without any specific legislative authority. Active dissemination of personal information may be undertaken through intranet or extranet applications provided that:

- there are adequate authentication procedures to ensure that individuals or their authorized representatives are requesting the personal information; and
- there is reasonable security surrounding the communication of the electronic data.

Such disclosure is usually done where a considerable demand occurs for a particular type of record. Making the process more routine, with fewer process and approval requirements, can save the school jurisdiction considerable time, effort and resources.

***Strategy***

To the extent possible, provide means outside the *FOIPP Act* for individuals to access and, if necessary, seek correction of personal information about themselves. The same rules under Section 83 of the *FOIPP Act* apply. Normally, the non-FOIPP process should provide the same personal information as if the individual had made a FOIPP request. If individuals may receive more information about themselves through the FOIPP process, they must be advised that this is the case.

***Strategy***

When establishing information networks with public modules, consider the feasibility of incorporating authentication, encryption and other electronic commerce and security features that will enable you to undertake transactions involving individuals obtaining personal information about themselves from the system on a routine basis.

***Basic Questions***

To the extent that information technology is used to maintain student, employee and other such personal information, the following questions related to systems design and implementation are relevant.

- ❑ Have we identified all categories of personal information where we are required or empowered to release such information to the individual it is about or to another authorized person?
- ❑ Can we use routine disclosure methods combined with information technology applications to improve and simplify such access?
- ❑ Can we ensure through technical means that only the entitled individual or an authorized representative has access to the specific personal information about the individual?
- ❑ Are adequate safeguards in place to protect the personal information within the electronic system and during its communication?
- ❑ Are there non-FOIPP means by which someone can request correction or amendment of a record within the system?

## PROTECTING PERSONAL PRIVACY

Part 2 of the *FOIPP Act* establishes controls relating to the collection, accuracy, retention, protection, use and disclosure of personal information. These controls are known as fair information practices. Personal information is defined as recorded information about an identifiable individual. Thus, it could be information about students, parents, guardians, contact individuals, teachers, employees or contracted personnel.

### WHAT IS PRIVACY?

Public polling in Canada has revealed a high concern (as high as eighty per cent) among individuals that they have lost control over how their personal information is used and to whom it is disclosed in the emerging information society. This concept, known as informational privacy, is dealt with in Part 2 of the *FOIPP Act*. It is defined as the right of individuals to determine when, how and to what extent they will share personal information about themselves with others. School jurisdictions have long operated on the principle of *confidentiality* but privacy is a broader concept.

### PRIVACY REQUIREMENTS

Part 2 of the *FOIPP Act* contains a *code of fair information practices* for the protection of privacy. In general terms, it requires school jurisdictions to:

- establish an information privacy principle as part of their overall administration;
- obtain and keep only information that is directly related to a program or activity or

purposes consistent with it;

- in most instances, tell the individual why they are collecting information and the uses and disclosures to which it will be put;
- use personal information only for the original purposes for which it has been collected, a use consistent with those purposes or a use for which personal information may be disclosed to the school jurisdiction under Section 38 of the *FOIPP Act*;
- permit only disclosures of personal information that are in accordance with Sections 38, 40 and 41 of the *FOIPP Act*;
- take reasonable measures to protect personal information from theft, loss, and unauthorized use or disclosure;
- meet the right of individuals to access and to correct or annotate (i.e., place a disclaimer on the record or flag the data) the information held about them; and
- ensure that all these privacy requirements are included in any new applications of technology or systems which hold or process personal information.

## IMPLEMENTING PRIVACY PROTECTION FOR INFORMATION SYSTEMS

As indicated above, Part 2 of the *FOIPP Act* establishes controls over personal information in order to protect individual privacy. These fair information practices are largely based on a special life-cycle approach to the management of personal information.

This forms a sub-set of the life-cycle for information management that underpins both technology management and modern electronic record-keeping. It requires that privacy issues relating to the collection and compilation, completeness and accuracy, protection, use, disclosure and retention of personal information be integrated into the systems development and implementation processes of an organization.

***Strategy***

Develop corporate privacy protection policies and procedures that enable you to:

- establish a methodology for addressing privacy protection and related security issues in planning and establishing functional specifications for new or modified personal information systems;
- review personal information systems and bring them into compliance with Part 2 of the *FOIPP Act*;
- review forms used in the collection of personal information to ensure that they meet the collection and notification requirements of the *FOIPP Act*;
- establish a security policy which includes protection of privacy as one of its aspects; and
- identify and manage the data matching of personal information.

## PLANNING NEW AND MODIFIED PERSONAL INFORMATION SYSTEMS

The privacy protection requirements set out in Part 2 of the *FOIPP Act* should be fully integrated into the design, construction and implementation of computerized information systems used to process personal information.

Quality management of technology should go hand in hand with privacy protection.

***Strategy***

Establish practices and procedures which provide for the consideration of the requirements of Part 2 of the *FOIPP Act* in the planning, design, development of specifications and implementation of information technology to new or modified information systems used to collect, compile, process, store, use, disclose or manipulate personal information.

***Strategy***

Require that a privacy impact assessment (PIA) forms part of the authorization for all information systems used to collect, compile, process, store, use, disclose or manipulate personal information. This document should be the basis for attesting to the superintendent that measures have been integrated into the information system to meet the requirements of Part 2 of the *FOIPP Act*. (A model form is provided in Part 5 of this study.)

## PRIVACY IMPACT ASSESSMENT

A privacy impact assessment (PIA) is simply a systematic approach to assessing the legal requirements of Part 2 of the *FOIPP Act*. The approach is important for school jurisdictions because they hold a great deal of relatively sensitive personal information. Public confidence is related, in part, to an organization's ability to protect such information. At the same time, it is important that privacy protection not become a major barrier to accomplishing the core goal of providing quality educational services. The PIA can serve as a tool for ensuring that reasonable and adequate measures are taken to protect the privacy of individuals whose information is processed and available on a personal information system while adapting such measures to the milieu and business needs of the educational organization.

A PIA is best carried out during the systems design process. It should involve joint analysis by the FOIPP co-ordinator, the information technology representative and the program area for which the system is being developed. A detailed methodology for a PIA is provided in Part 5 of this study.

## REVIEW OF EXISTING PERSONAL INFORMATION SYSTEMS

**Strategy**

Establish policies and organizational structures that will facilitate the integration of privacy protection requirements and practices into the ongoing management of personal information systems and plan how to bring existing program activities and personal information systems into compliance with Part 2 of the *FOIPP Act*.

This will involve a review of existing information systems used to collect or compile, process, use, disclose, store or manipulate personal information. Since this may be a large task, remedial measures should be planned and implemented over a reasonable number of years. A checklist for reviewing existing personal information systems is provided in Part 5 of this study.

## DATA MATCHING

Data matching is defined as the comparison of personal data obtained from different sources, including both electronic and paper-based formats, for the purpose of making decisions about individuals to whom the data pertains. Data matching is therefore an activity involving the collection, use and disclosure of personal information. Included in the definition of data matching is data linkage, also known as data profiling.

Data matching plays a valuable role in increasing the efficiency of a wide variety of government programs. However, it also can have a major impact on the privacy of individuals in the information that they provide to the provincial government. For this reason, there is a need to balance the requirements for efficiency and effectiveness in government programs with the potentially invasive nature of the activity.

**Strategy**

Require that all data matching activities involving personal information be reviewed by the jurisdiction's FOIPP co-ordinator and, where appropriate, that advice be sought from the Office of the Information and Privacy Commissioner.

***Basic Questions***

In considering the implementation of the privacy protection requirements in Part 2 of the *FOIPP Act* for electronic information systems which store, manage, manipulate or communicate personal information, the following questions are pertinent.

- ❑ Is there a process in place to ensure that a PIA is conducted during the development of new and modified information systems?
- ❑ When a PIA is conducted, are we satisfied with the measures recommended to ensure the system meets the legal requirements of Part 2 of the *FOIPP Act*?
- ❑ Is this technology project of such a significant and/or innovative nature that it merits consultation with the Information and Privacy Commissioner?
- ❑ Is a process and reasonable schedule in place to undertake the review of existing information systems dealing with personal information and any related forms to ensure that each system is brought into compliance with the requirements of Part 2 of the *FOIPP Act*?
- ❑ Are all program areas and schools identifying all data matching referred to the FOIPP co-ordinator for review and approval?

## FOIPP AND INFORMATION MANAGEMENT

### MANAGING ELECTRONIC RECORDS

Sound information management is essential to the effective administration of FOIPP. The access rights to the records provided in the *FOIPP Act* are intended to make public bodies more open and accountable to the public. Inadequate record-keeping can result in the inability to find records, failure to adequately document events and transactions, failure to control destruction of records, and inadequate systems on which to carry out routine disclosure and meet legal privacy protection requirements.

***Strategy***

Ensure that the management of all recorded information in your organization, including electronic information, is governed by a corporate information management policy. This should be developed with the administration of FOIPP in mind and include appropriate references to FOIPP requirements in both the policy statements and the procedures, practices and standards used to implement the policy.

### Basic Questions

The following questions are relevant to FOIPP and information management issues.

- □ Does our organization have in place an information management policy that:
  - applies to all records;
  - is based on the management of information as a corporate resource;
  - adopts a life-cycle management approach; and
  - assigns accountability for record-keeping systems?
- □ Does our organization have effective management and operational mechanisms for:
  - supporting life-cycle management of information;
  - establishing and maintaining record-keeping systems;
  - organizing and filing electronic records;
  - establishing and maintaining a corporate inventory;
  - governing the creation and generation of records;
  - establishing a standard for transitory records;
  - dealing with the organization, retrieval and storage of recorded information;
  - planning information systems;
  - governing the disposition of recorded information, including electronic information; and
  - managing information provided to contractors or which is required to be maintained by contractors?

## SECURITY

In order for information systems to comply with the varying components of the *FOIPP Act*, there are technical security and awareness issues that must be appropriately managed. This study does not include a technical discussion of security issues and approaches. Rather, it deals with management approaches and tools which will assist both the administration of effective security measures and the ability to meet FOIPP requirements, particularly those relating to the protection of personal information.

An essential first step in governing the development of security measures is to develop a security policy or administrative framework that sets out the requirements and expectations of senior management in regard to security. This should incorporate FOIPP requirements, particularly the need to protect personal information throughout its life-cycle, from its creation to its disposal, and from the earliest stages of the systems development life-cycle to ensure that such information systems reflect legal and policy requirements relating to privacy.

***Strategy***

Develop a security policy or administrative framework to govern protection of information and other assets within your school jurisdiction and to communicate security expectations and requirements to officials, staff and teachers. Policy requirements should be based on a technical security accountability framework. A technical security audit methodology should be planned as well as a methodology for assessing threats and risks. An assessment should be done of the current methods applied to installed technologies and the database collections of information.

***Basic Questions***

In dealing with security of information, particularly personal information, the following questions are relevant.

- ❑ Do we have a comprehensive security policy in place to govern activities related to the availability, confidentiality and integrity of our information systems?
- ❑ Do we integrate security assessments designed to aid in the protection of personal privacy into the planning and design specifications of new or modified systems dealing with personal information?
- ❑ Is responsibility and accountability for the management of security issues and implementation of protective measures effectively assigned within our organization?
- ❑ Do we use a threat-and-risk assessment approach to determine the nature and extent of protective measures required for information systems?
- ❑ Do we assess the security risks and take effective measures to protect our internal systems from penetration by external users through our own public access systems and interactive networks such as the Internet which are used by our employees and students?

## E-MAIL

Electronic mail, or e-mail, is a digital form of communication that allows messages and documents to be sent from one computer to another. It is fast becoming a major tool by which officials, employees and teachers communicate among themselves. It is used extensively by students and is now, in some instances, being expanded into a two-way communication with the public over the Internet.

It is necessary to control official records of the school jurisdiction, which may reside on e-mail systems. These may well become the subject of a FOIPP request and may have to be produced for the applicant, unless they have been disposed of under an approved records schedule. There also are privacy protection issues arising from the use of e-mail. One involves such a system's use to transmit sensitive personal information without proper security measures. The second involves the surreptitious monitoring of the personal e-mail of teachers, employees or students without a strong legal case for suspecting wrong-doing.

**_Strategy_**

Develop a policy on the use and management of e-mail for your organization, which takes into account the requirements of the *FOIPP Act*.

**_Basic Questions_**

The following questions are relevant to e-mail management.

- □ Does our organization have in place effective policy and procedures to manage the e-mail system in line with the requirements of the *FOIPP Act*?
- □ Do staff, teachers and students understand the purpose and rules which govern e-mail systems in our jurisdiction and how and under what circumstances e-mail records may be deleted from the system?
- □ Do we have FOIPP procedures that provide for the routine search of e-mail systems when locating records responsive to a FOIPP request?
- □ Do staff and teachers understand the rules about communicating sensitive personal information by e-mail?

# PART 2: INTRODUCTION

The *Freedom of Information and Protection of Privacy (FOIPP) Act* came into effect for school jurisdictions on September 1, 1998. The provisions of the legislation have a profound impact on how schools and school jurisdictions will apply and use information technology in the future, both in regard to accessing information and protecting individual privacy. This study is intended to help school administrators, FOIPP personnel and those involved in developing and implementing electronic systems to better understand the *FOIPP Act* as it relates to the application of information technologies and to aid them in devising strategies and approaches to effectively deal with its requirements.

The study is oriented toward technology perspectives, but a good portion of the discussion and approaches are applicable to wider FOIPP matters.

## SCOPE OF THE *FOIPP ACT*

The *FOIPP Act* expresses the following five basic purposes that can affect the application and use of information technology in school organizations.

1. *Right of access:* The *FOIPP Act* allows any person a right of access to the records in the custody or under the control of a school jurisdiction subject to limited and specific exceptions.

2. *Right of access to information about oneself:* The *FOIPP Act* allows individuals, again subject to limited and specific exceptions, a right of access to personal information about themselves held by a school jurisdiction.

3. *Right of correction:* The *FOIPP Act* allows individuals a right to request corrections to personal information about themselves that is held by a public body.

4. *Protection of informational privacy:* The *FOIPP Act* requires school jurisdictions to control the manner in which they collect personal information from individuals, to control the use and disclosure of such information and to take reasonable measures to ensure that it is accurate and secure.

5. *Independent review:* The *FOIPP Act* provides that all decisions made by school jurisdictions under the legislation may be reviewed by the Office of the Information and Privacy Commissioner and any complaints resolved by the Commissioner. This means that the Commissioner may review decisions to refuse access to information or questions regarding the collection, use, disclosure, accuracy and protection of personal information. The Office, with or without a complaint, may investigate or audit personal information systems or comment on the impact of a by-law or resolution of the board or of an operational or administrative decision with regard to freedom of information or protection of privacy.

These purposes have an impact on the application of information technology in school jurisdictions in four basic domains:

- accessing of general information;
- students, parents and employees accessing personal information about themselves;
- protection of privacy in the development and management of electronic information systems that deal with personal information; and
- the overall management and protection of the information resources of school jurisdictions.

Each of these domains is discussed below and major issues addressed. Useful questions for officials, employees and teachers when dealing with FOIPP and technology applications are provided for each domain. These are designed to act as signposts to strategies and approaches that can support both successful administration and management of the access and privacy legislation and innovative and effective application of information technology. The basic strategies and questions are summarized in the Overview and Checklist for Senior Managers, which forms Part 1 of this study.

## DEFINITIONS

Several important definitions are important for understanding the strategies and approaches included in this study.

*Applicant* means any person who makes a request under the *FOIPP Act*. There is no limitation on who may make a FOIPP request. Any individual, corporation or other organization either inside or outside Alberta may make a request.

*Custody* of a record means physical possession; for example, the electronic record is on a system in the school jurisdiction or in an off-site storage facility.

*Control* of a record means that the school jurisdiction has the authority to manage, restrict, regulate or administer the use, disclosure and disposition of the record. The most common situation where an organization may have control of a record is in the case of contracted services. Electronic records may be in the custody of the contractor but under the control of the school jurisdiction.

*Personal information* means recorded information about an identifiable individual (for example, name, address, date of birth, age, sex, religion, blood type, opinions), including anyone else's opinions about the individual.

*Record* means a record of information in any form. A FOIPP request may deal only with records. The definition of "record" includes electronic documents and electronic messages and notes and draft material created in carrying out school jurisdiction business but it does not include software or any mechanism that produces records.

Certain classes of records are excluded from the coverage of the *FOIPP Act*. The most relevant to school jurisdictions are:

- a question that is to be used on an examination or test;
- a record made from a registry operated by a public body where public access to the registry is normally permitted; and
- a record of an elected school official that is not in the custody or under the control of the school jurisdiction.

Advice about what recorded information may be excluded from the coverage of the *FOIPP Act* should be sought from the jurisdiction's FOIPP co-ordinator on a case-by-case basis.

Other definitions may be found in Section 1(1) of the *FOIPP Act* and in the appropriate parts of this study.

# PART 3: ACCESSING GENERAL INFORMATION

## INTRODUCTION

Each school jurisdiction should have in place a FOIPP policy, which includes practices and procedures for responding to requests made by applicants under the *FOIPP Act*. The nature and extent of such a policy is beyond the scope of this study.

Such a policy will, however, have an impact on the management of information technology to the extent that all information in the custody or under the control of a school jurisdiction will be considered a record for purposes of the *FOIPP Act* and thus could be subject to FOIPP requests. As indicated in Section 1(1)(q), only software or any mechanisms used to produce records are excluded from the definition of record. Thus, searches for records responsive to requests must include any pertinent sources of electronic records (databases, correspondence systems, electronic mail, etc.) The appropriate management of electronic records and e-mail to meet FOIPP requirements is discussed in Part 6 of this study.

An important feature of the *FOIPP Act* is the requirement that a school jurisdiction create a record for an applicant if:

- the record can be created from a record that is in electronic form and in the custody or under the control of the public body, using its normal computer hardware and software and technical expertise; and
- as stated in Section 9(2), creating the record would not unreasonably interfere with the operations of the public body.

*Unreasonable interference* is a relatively difficult test to meet. A school jurisdiction would have to show, for instance, that its computer capacity is fully employed throughout a whole 24-hour cycle and the processing would unduly disrupt work. Or, it might be able to demonstrate that only a certain amount of money is allotted to information processing and this could not be recouped through the processing of the FOIPP request. This would mean that resources would not be available to carry on the organization's basic operations.

However, to the extent that school jurisdictions use technology to process and manipulate non-personal information to analyze their operations, there may be FOIPP requests from interested individuals and groups to produce information in forms and formats which are useful to them. They then may use this information to monitor and critique various school operations and policies.

It is fair to say that FOIPP requests are both expensive and time consuming to process and are sometimes confrontational in nature. For these reasons, FOIPP requests should be viewed as the avenue of last resort in dealing with persons who may wish to obtain information about schools or school administration. It is very important to have an information access policy for the school jurisdiction, which is paramount to its FOIPP policy and governs the operation of the latter. For this information access policy, appropriate and innovative application of information technologies can play a critical role.

***Strategy***

Continue and strengthen current methods of communicating with students, parents, employees and the public-at-large, and seek to expand this informal, non-FOIPP approach to providing information. Develop an information access policy that enables your organization to be proactive in providing access to information and to avoid reacting to demands for information through FOIPP requests.

Section 83 of the *FOIPP Act* enables this approach. It provides that a school jurisdiction may specify categories of records in its custody or under its control that are available to the public without a FOIPP request. If a FOIPP request comes in for such information, the requester can be referred to the non-FOIPP process, provided s/he will obtain all the information requested.

In addition, Section 83(2) permits the school jurisdiction to establish a fee schedule for such information under its own authorities (i.e., the *School Act*) and separate from the FOIPP fees. There are no legislated criteria for such a fee structure and it may be adjusted to the business approaches and needs of the school jurisdiction.

Further, Section 84 of the *FOIPP Act* requires a school jurisdiction to make available to the public all manuals, handbooks or other such guidelines used in decision-making processes that affect the public in the administration of programs or the carrying out of programs or activities.

## POLICY PRINCIPLES FOR AN INFORMATION ACCESS POLICY

It is important that everyone involved understand an organization's commitment to providing a wide range of useful information outside the *FOIPP Act*. Fundamental policy principles for an open and accountable administration might read as follows:

- We will continue to provide information to students, parents and the public. The *FOIPP Act* does not replace existing procedures for public access to information or records of this organization.
- We are an open and accountable organization. Therefore, in the future, we will attempt to meet all requests for information or records, including those requested under the *FOIPP Act*, through routine disclosure and active dissemination without resort to the formal procedures of the legislation. Use of the *FOIPP Act* should be viewed as the last resort for a person seeking information or records.
- When disclosing information, we will ensure protection of the privacy of individuals, the rights of businesses and other groups dealing with our

organization and protection of other confidential information relating to the effective operation of our organization that is in the public's interest.

- When it is necessary to respond to a FOIPP request for records, our organization will meet all the requirements, duties and obligations of the *FOIPP Act* in an efficient and effective manner and will make every reasonable effort to assist applicants and respond in an open, accurate and complete manner as set out in Section 9(1) of the legislation.

The information access policy also should establish strategies and approaches to routine disclosure and active dissemination as outlined below. To the greatest extent possible, new applications of information technology should incorporate public access modules or features.

***Strategy***

To the extent possible and where it is practical, employ information technology to support regular disclosure of information outside the FOIPP process in order to better meet educational objectives and avoid FOIPP requests, while implementing the spirit of the *FOIPP Act* for more open, accountable and transparent administration of school jurisdictions.

There are two distinct approaches to broadening disclosure of information outside the *FOIPP Act*—routine disclosure and active dissemination.

*Routine disclosure or disclosure without a FOIPP request* occurs when access to a record can be granted without resort to a request under the *FOIPP Act.*

*Active dissemination* occurs when information or records are periodically released (without any request) under a program or release strategy. This is best used where there is a strong and constant demand for information that would be available to the public.

Excellent candidates for such types of non-FOIPP disclosures are situations where:

- disclosure is mandated by another statute or by-law and the records will be released;
- no exceptions (i.e., the *FOIPP Act* has no provision for refusing access) apply to records;
- no mandatory exceptions apply to a class of records (i.e., the *FOIPP Act* requires that access be refused) and the school jurisdiction has decided not to invoke any discretionary exceptions; or
- exceptions apply to a class of records but the sensitive information can easily be suppressed from information that then may be routinely disclosed.

An example of this type of approach is the dissemination of annual school and systems profiles by the North York Board of Education. To quote the board's public affairs officer, Ross Parry:

> A strong belief in an open, honest, and accountable approach to communicating with parents and the public has led the North York Board of Education (the Board) to release a massive amount of data that is contained in its annual School and System Profiles. The disclosure of the information is a benchmark achievement.
>
> Unprecedented in Canada, these reports monitor the knowledge and skills of students in the North York public school system in mathematics and literacy, including reading, writing, spelling and grammar. The results of the tests help the Board to plan for improvement in student achievement; the results also help educators and parents determine how well students are meeting the curriculum objectives. But by far the most important aspect is that these published results of the testing program give greater accountability to parents/taxpayers for the performance of students and the whole school system.
>
> In March, 1995, parents received a school profile for their child's school. This short, plain language profile included: an overview of the school's programs, facilities, curriculum highlights and other general information; demographic information on students; results from annual board tests in mathematics and literacy and the Ministry of Education and Training's Grade 9 reading and writing test; a standard explanation of the tests; the school's own comments on their test results, including a summary of the school's improvement plans; and a summary of system-wide results so that parents could compare their child's school results, relative to the whole system. Parents also received a short "system profile" that gives the test results and demographic data on a system-wide basis for all schools of the same type. Two other information brochures also accompanied the package to increase understanding and provide a context to the data.
>
> A combination of inter-related factors led up to the decision to break from the tradition of secrecy surrounding school test results and move to a routine release of school-by-school test results:
>
> - Parents' demand for more accountability was escalating.
> - The media were critical of school boards for concealing information and for poor accountability to parents.
> - Complaints from taxpayers over some school boards charging, in some cases, large "administrative" fees to access school-by-school test results.
> - In July, 1992, the IPC (Ontario Information and Privacy Commissioner) issued Order M-27. The Board considered this to be a landmark ruling.
>
> In this order the institution (a school board) was ordered to disclose two records which identified particular schools by name. The appellant had

requested access to records that showed the standings of the institution's schools in provincial reviews for Grade 11 and 12 physics and chemistry (1987 to 1988) and Grade 9 geography (1986 to 1987); and the results, both school-by-school and board-wide, of all system-wide tests given since 1983 in English, mathematics and science courses for Grades 9 to 12 and Ontario Academic Credits.

The institution granted access to five responsive records, but the records sent to the appellant identified each school not by name, but by an alphabetical code designation. The subject of the appeal was the institution's decision not to identify each school by name.

The institution was ordered to disclose two records that identified the schools by name. The school name and its alphabetical code are not the personal information of any identifiable individual, and it was not reasonable to expect that the economic interests or the competitive position of the institution would be prejudiced by the disclosure of the record.

- The Ministry of Education and Training has indicated that all Ontario school boards will be required to administer province-wide tests by 1997 in at least two, and perhaps four grades, covering mathematics and literacy. The type of tests and how the tests will be reported to parents and the public is yet to be determined.
- After eight years of developing its testing program, the Board was well-positioned to release school-by-school results.

Over several months, the method of reporting school-by-school results was developed through extensive consultation with teachers and principals and focus groups with parents and students. By March, 1995, 4000 teachers had received their school's profile, the system profile for their school type and two companion brochures. Each school received a binder containing the profiles for all 130 schools within the Board. The binders were placed in all North York Public Libraries and distribution to parents was carried out.

For more details, see *Enhancing Access to Information: RD/AD Success Stories,* A Joint Project of the Information and Privacy Commissioner/Ontario and the Freedom of Information and Protection of Privacy Office, Public Access Services Branch of Management Board Secretariat/Ontario, available at URL <http://www.ipc.on.ca/default.HTM>.

In this case, the work to promote increased disclosure outside FOIPP was considerable. It was considered necessary and appropriate, however, to meet more general educational needs, as well as avoiding on-going FOIPP requests. The dissemination approach in this case was paper-based; however, with the rapidly developing network and communications technologies it could, perhaps, now be more easily accomplished through the application of information technology.

The establishment of new or modified electronic information systems, including an Internet site for an organization, provides an avenue for establishing mechanisms where routine access or active dissemination may be considered. Initially the impetus may come from a variety of external sources:

- demand from parents for more accountability;
- media reports critical of school jurisdictions for concealing information and not being accountable to parents;
- complaints from taxpayers about high fees for preparing customized information reports; or
- a burgeoning number of FOIPP requests and orders from the Information and Privacy Commissioner that result in large amounts of information being released through the *FOIPP Act* at considerable cost to the school jurisdiction.

**Strategy**

Use electronic media and formats, including public networks, as appropriate and within budgetary constraints, in order to make information more easily accessible and useful to students, parents and the public. Such efforts, however, should not preclude those without access to computer technologies from accessing similar information by other means; for example, publications, library sources, etc.

## PRACTICES FOR ROUTINE DISCLOSURE/ACTIVE DISSEMINATION

Routine disclosure and active dissemination (RD/AD) should become a normal part of your organization's operations and a support for improving its performance. To the extent possible, information technology should be used to accomplish this goal.

As the North York example indicates, the issue of open access to information goes well beyond the requirements of FOIPP. School jurisdictions face major challenges in meeting the public's growing need for information and demand for related client services in a cost-effective fashion. To help satisfy this demand and foster more open public administration, the following practices to support *routine disclosure* and *active dissemination* are suggested.

1. *Review of information holdings:* In starting to establish a system of *routine disclosure* and *active dissemination*, it is necessary to review the records of the public body to determine where the concepts may apply.

   A good starting point for a school jurisdiction is the preparation of the entries for the *Local Public Body Directory of Records*. These entries should form the basis for a review and survey of record holdings and electronic information systems to determine what types of information could be provided to the public routinely or actively disseminated to client groups. The findings of the review can serve as the basis of a basic inventory of information holdings. As indicated in Part 6, this is a crucial tool for information management in the emerging electronic work environment. The following chart can aid in reviewing information holdings, both electronic and in paper and other formats. The results should be entered into an information holdings database and updated as new systems or categories of information holdings are established.

## CHART 1
## CHECKLIST FOR ASSESSING CURRENT INFORMATION HOLDINGS

| Control No. | Description of Information System/Group | Types of Information Obtained or Created | Location of Information | FOIPP Exceptions That May Apply | Status for RD/AD |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Release and dissemination can take several forms, such as:

- release of particular information whenever a student, parent or other member of the public requests it as part of the service being offered;
- use of information and document centres to provide information, including access terminals and mail and fax services for information;
- use of reference databases to answer frequently asked questions from students, parents and the public;
- publication of self-browse and self-service database services;
- distribution of databases to libraries and other public facilities or use of private sector information services to mount popular public databases; and
- use of the Internet and other public networks to distribute information.

A list of public information sources for the school jurisdiction should be prepared, kept up-to-date and distributed to all officials, employees and teachers who may deal with inquiries from students, parents or the public. This list also should be generally available, including school Internet sites, where they exist. Such information should never be dealt with under the access provisions of the *FOIPP Act*.

2. *Co-ordinating committee:* Where a school jurisdiction is larger in size or decentralized in operation, it may be advantageous to develop a network of contacts in program and administrative areas. This may be built into a co-ordinating group that is mandated to develop a corporate approach on routine disclosure and active dissemination and to help implement such disclosure practices.

Members of such a group should include:

- the FOIPP co-ordinator who can assist in interpreting the *FOIPP Act*;
- interested staff and teachers with information that may well qualify for routine disclosure and active dissemination;
- a communications officer involved in information release and dissemination; and
- a representative from the information technology area, who understands how the public body can use the new information networks to release and disseminate information.

Either the FOIPP co-ordinator or the committee should develop a corporate approach to routine disclosure and active dissemination, which may be incorporated in the information access policy.

3. *Review of inquiries:* The FOIPP co-ordinator or the committee should review the types of requests currently made to the school jurisdiction to determine if these can be met through either routine disclosure or active dissemination. The objective should be to prevent, to the greatest degree possible, these informal requests turning into formal requests under the *FOIPP Act*. This should involve ongoing monitoring and review of formal access requests to determine whether requests of a particular nature can be handled under informal practices.

4. *Delegation of authority:* The organization should establish structures to ensure that routine disclosure and active dissemination are considered for all programs and services where they might be applicable and effective. All areas should be required to delegate all disclosure without request to the program area where the information is collected, compiled or created. The program area should be required to establish mechanisms to assure the rapid and effective release of the information, in accordance with the corporate policy on routine disclosure and active dissemination.

## CREATION OF NEW INFORMATION SYSTEMS

The information access policy should require that the FOIPP co-ordinator be consulted when there are plans to create new information systems within the school jurisdiction. This consultation should determine whether or not any of the new information could be released outside the *FOIPP Act*.

Consideration should be given, where possible, to modifying standard records by removing segments that would be subject to mandatory exceptions.

For example, if a record contains both general information and personal information, but the main purpose of the record is to provide general information, then practices can be put in place to suppress the fields for personal information in an electronic record. This may make the record available for either routine disclosure or active dissemination.

## ACTIVE DISSEMINATION

Active dissemination can take many forms. As indicated above, a school jurisdiction may have an information centre for students and parents where information can be gathered rapidly and sent to them, either by mail, modem or fax.

School jurisdictions also are establishing Internet sites. These sites can hold public information that can be accessed by students, parents and the public. Such access can be obtained either through an intermediary or by direct on-line access, if users have the equipment and expertise.

In other instances, schools can use other public or private agencies, including libraries or non-profit organizations, which are part of their clientele, or general information services to distribute information on their behalf.

All active dissemination projects involve some investment by school jurisdictions and these costs have to be balanced against improved services to students, parents and the public and possible avoidance of FOIPP requests.

When considering dissemination of electronic products, public bodies should, whenever appropriate and within budgetary constraints, consider using public and local networks such as the Internet, freenets and civic networks. Such systems need to be designed following the structured information technology security considerations set out in Part 6 of this study.

### Basic Questions

The following questions should be posed to the organization when dealing with issues over access to information.

- ❑ Does our organization currently have in its custody or under its control information that:
  - is in demand; and
  - the release of which in a proactive and informal manner would better meet the concerns of students, parents and the public for more open and accountable governance of our school, board or district?
- ❑ Could we release such information either on a routine basis or through active dissemination without compromising those mandatory interests, particularly personal privacy, which we are required to protect under the *FOIPP Act*?
- ❑ Do the current technology applications which we are undertaking or planning to undertake in the near future, including use of the Internet, adequately take into account the need for the routine disclosure or active dissemination of this type of substantive organizational records?
- ❑ Have we or are we going to automate the creation and management of our organization's manuals, handbooks or other guidelines that the *FOIPP Act* requires must be made available to the public? Have we recognized this requirement as part of the management application?
- ❑ Do we have an information access policy and an ongoing process in place to identify such sources of information and to ensure that they are made available in ways that meet our overall business objectives?
- ❑ Do we release such information in forms (electronic and paper) which meet the needs of students, parents and the public?
- ❑ To the extent that we permit public access to electronic information (for example, an Internet site), do we have adequate technical safeguards in place to ensure that no access is permitted to our electronic information systems beyond these public data sources?

# PART 4: ACCESSING PERSONAL INFORMATION

The *FOIPP Act* provides that individuals or their representatives may access personal information, subject to limited and specific exceptions. There are fewer exceptions to access that apply to situations where individuals are requesting access to information about themselves. As well, fairness dictates that such information is provided to them unless there are very strong reasons why access should be refused; for example, the information may harm the physical or mental health of the applicant.

Although personal information forms a special category of information, it too should, to the greatest extent possible, be considered for disclosure through routine channels.

School jurisdictions may be able to identify categories of records containing personal information that may be made available routinely **only to the individual** that the information is about. This may be done without any specific legislative authority. Active dissemination of personal information may be undertaken through intranet or extranet applications provided that:

- there are adequate authentication procedures to ensure that individuals or their authorized representatives are requesting the personal information; and
- there is reasonable security surrounding the communication of the electronic data.

These factors are discussed further in Parts 5 and 6 of this study.

Such disclosure is usually done where a considerable demand occurs for a particular type of record. Making the process more routine, with fewer process and approval requirements, can save the school jurisdiction considerable time, effort and resources.

The *School Act* (Section 18) provides for the creation of the Student Record and establishes processes for the review and correction of the record. The *Student Record Regulation* governs the content of the record, its retention and who may have access to it. The student, the student's parents (except for independent students) or any other individual who has access to the student pursuant to a separation agreement or an order of the court can review the record. In determining who may review the Student Record, reference needs to be made to the definitions of independent student and parent set out in Sections 1(1)(h), and 1(2) of the *School Act* and the rights of independent students in Section 1(3). Section 103(2.2) of the *School Act* permits anyone who reviews a student record under Section 18 to appeal to a board a decision of an employee of the board in regard to accessing or to the accuracy or completeness of the Student Record. This is a process which occurs outside the correction procedures established by the *FOIPP Act* and which could continue to be used as a direct appeal process. Those access processes remain in place and, to the extent possible, may be enhanced through the use of information technology. Where this is the case, the technical requirements for authentication and communications security apply and any technology application should be subjected to a privacy impact assessment (PIA) as discussed in Part 5 of this study.

There may be other personal information about a student or the student's parents in the school jurisdiction's files. Again, except to the extent of meeting mandatory exception criteria set out in the *FOIPP Act*, such personal information should be made available to the individuals it is about in a routine manner.

Routine access also should apply to most employee records. An exception here may be disciplinary files where information about the investigation process, other individuals and confidential sources may need to be protected.

Section 83(2) of the *FOIPP Act* permits the establishment of a fee for providing such information to individuals and, if a process for dealing with requests for information outside the *FOIPP Act* is put in place, individuals who make formal requests can be referred to it. For instance, a flat fee could be established to apply when individuals are obtaining their transcripts.

In instances where the *School Act* or other legislation does not govern access, individuals must be given the choice of either accepting the non-FOIPP process or making a request under the *FOIPP Act*. Normally, they will opt for the routine process unless they have a specific grievance with the organization and wish to exercise their legal rights.

Normally, the routine disclosure process should be used only when individuals will receive exactly the same information that they would under a FOIPP request. Where this is not the case, public bodies should explain what types of personal information will not be released and give the individual the option of making a FOIPP request.

If a fee is charged for individuals to access personal information about themselves, this fee should normally cover only the cost of duplicating the information.

It is most practical to combine the identification of personal information banks (PIBs) required under Section 82(6) of the *FOIPP Act* with a review of what personal information can be made available to the individuals to whom it relates on a routine basis outside the FOIPP process. It would be most advantageous to store this listing of PIBs in a database and keep it up to date as new personal information systems are developed. The following chart can aid in this process of identifying PIBs and planning routine access to personal information by the individuals it is about, both currently and for future applications of technology.

## CHART 2
## IDENTIFICATION OF PIBS AND ROUTINE DISCLOSURES OF PERSONAL INFORMATION

| Control No. | Tasks | Analysis |
|---|---|---|
| | Description of personal information system | |
| | Nature of records (electronic, paper, photos, etc.) | |
| | Description of personal information collected or compiled | |
| | Categories of individuals covered by the system | |
| | Authority for collection | |
| | Location of information | |
| | Current disclosures to other organizations | |
| | Current access by individual | |
| | Potential for RD/AD | |

### *Strategy*

To the extent possible, provide means outside the *FOIPP Act* for individuals to access and, if necessary, seek correction of personal information about themselves. The same rules under Section 83 of the *FOIPP Act* apply. Normally, the non-FOIPP process should provide the same personal information as if the individual had made a FOIPP request. If individuals may receive more information about themselves through the FOIPP process, they must be advised that this is the case.

### *Strategy*

When establishing information networks with public modules, consider the feasibility of incorporating authentication, encryption and other electronic commerce and security features that will enable you to undertake transactions involving individuals obtaining personal information about themselves from the system on a routine basis.

### *Basic Questions*

To the extent that information technology is used to maintain student, employee and other such personal information, the following questions related to systems design and implementation are relevant.

- ❑ Have we identified all categories of personal information where we are required or empowered to release such information to the individual it is about or to another authorized person?
- ❑ Can we use routine disclosure methods combined with information technology applications to improve and simplify such access?
- ❑ Can we ensure through technical means that only the entitled individual or an authorized representative has access to the specific personal information about the individual?
- ❑ Are adequate safeguards in place to protect the personal information within the electronic system and during its communication?
- ❑ Are there non-FOIPP means by which someone can request correction or amendment of a record within the system?

# PART 5: PROTECTING PERSONAL PRIVACY

Part 2 of the *FOIPP Act* establishes controls relating to the collection, accuracy, retention, protection, use and disclosure of personal information. These controls are known as fair information practices. Personal information is defined as recorded information about an identifiable individual. Thus, it could be information about students, parents, guardians, contact individuals, teachers, employees or contracted personnel.

The *FOIPP Act* defines personal information as recorded information about an identifiable individual, including:

- the individual's name, home or business address or home or business telephone number;
- the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
- the individual's age, sex, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, blood type or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual, such as a performance report on an individual; and
- the individual's personal views or opinions, except if they are about someone else.

This is a non-inclusive list, and other categories of data may qualify as personal information.

## WHAT IS PRIVACY?

Privacy considerations are particularly important when information technology is applied to assist in the delivery of programs and services. Public polling in Canada has revealed a high concern (as high as eighty per cent) among individuals that they have lost control over how their personal information is used and to whom it is disclosed in the emerging information society. See, for example, Louis Harris and Associates, *Equifax-Harris Mid-decade Consumer Privacy Survey* (Atlanta, 1995) and Ekos Research, *Privacy Revealed: The Canadian Privacy Survey* (Toronto, 1993).

School jurisdictions have long operated on the principle of *confidentiality*. This is part of privacy protection, but privacy is a broader concept. As Ann Cavoukian and

Don Tapscott point out in their book, *Who Knows: Safeguarding Privacy in a Networked World* (Toronto, 1995):

> ...Privacy involves the right to exercise control over your personal information (e.g., its collection, use, accuracy, protection, retention and disclosure).... Confidentiality, on the other hand, provides only one means of protecting that information, in the form of keeping it secure from prying eyes.

Dr. Alan Westin, a leading international expert on privacy issues, sees the following privacy challenge for modern organizations in the processing, storage, use and manipulation and disclosure and communication of personal information (*Privacy and Freedom*, New York, 1967):

> Privacy has been adopted as the way to express the public's demand that powerful institutions engage in open, equitable, and procedurally fair relationships in dealing with individuals as consumers, employees and citizens. To do this, the public wants a better balance to be created between information subjects and information keepers in both the private and public areas, and especially where high technology systems are involved.

## PRIVACY REQUIREMENTS

Privacy protection requirements form a code of fair information practices relating to the collection, use, disclosure, accuracy and protection of personal information in the custody or under the control of a school jurisdiction. As well, there is a requirement to provide individuals with access to information about themselves and the means to correct or annotate such personal information. This latter aspect is dealt with in Part 3 of this study.

Part 2 of the *FOIPP Act* contains a *code of fair information practices* that creates the following obligations for school jurisdictions.

1. *An information privacy principle:* Individuals are entitled to privacy protection in all information systems under the custody and control of institutions.

   Information and other related technologies are tools to assist the delivery of various programs and services to individuals and *not* instruments to enable the collection and control of information which can be used for purposes other than those related specifically to the operation and administration of those programs and services.

2. *The need for principles for systems development:* School jurisdictions should assess the impact on personal privacy of planned activities or operations.

   School jurisdictions should take into account appropriate privacy protection measures in the planning and implementation of all new or modified personal information systems or technologies.

Individuals are to be informed about the development of new or modified personal information systems or technologies, particularly:

- the terms for participation,
- the consequences of refusal to participate,
- the nature of the personal information involved and how it will be protected, and
- the totality of the uses and disclosures contemplated.

3. *Information collection principles:* School jurisdictions must obtain and keep only information that is directly related to a program or activity operating under a specific or planned mandate, and the information must reasonably relate to that mandate or purposes consistent with it.

   Collection of information must be restricted to that which is directly related to a program or activity *and* is necessary for the operation of such programs or activities.

   Normally, school jurisdictions must tell the individual why they are collecting information and the uses and disclosures to which it will be put. There should be an understanding that the information will not be used for purposes other than those stipulated in the *FOIPP Act*, except with the informed consent of the individual concerned.

   Where information is collected through a more complicated process (for example, school registration), notification can take the form of a client brochure or other instrument or an explanation by a knowledgeable person.

4. *Principles of use:* School jurisdictions must use personal information only for the original purposes for which it has been collected, a use consistent with those purposes or a use for which personal information may be disclosed to the school jurisdiction under Section 38 of the *FOIPP Act*. Individuals must give informed consent for all other uses and must be able to withdraw that consent without penalty.

   Institutions must obtain and keep only information that could reasonably be expected to support current or planned activities. This does not preclude the retention of legal records, personnel and performance information, and historical data concerning a school jurisdiction, which must be retained over long periods of time for administrative purposes. It does, however, mean that during the collection process school jurisdictions must restrict collection to that personal information needed for administrative and operational purposes and not collect information that may be useful but has no immediate purpose.

5. *Principles of disclosure:* School jurisdictions must control all disclosures of personal information to ensure that they occur only in accordance with Sections 38, 40 and 41 of the *FOIPP Act*.

   The matching or linkage of data from two or more personal information systems for an administrative purpose directly affecting an individual must be carried out in accordance with the use and disclosure provisions of the *FOIPP Act*. Often an organization may wish to seek independent review of the proposal through the Information and Privacy Commissioner, who can assist in considering both the privacy and efficiency aspects of the data matching or linkage activity. Such multipurpose applications should be segregated to prevent possible merging or crossovers of personal information taking place in any transaction process.

6. *Information integrity, security and management principles:* Individuals must have confidence in personal information systems within school jurisdictions. To promote this confidence, institutions must continue the privacy protection measures commenced during the planning and operation of personal information systems by:

   - undertaking information management and technology practices and standards to assure that the information is accurate, timely, complete and relevant to the purposes for which it was collected or compiled;
   - ensuring that all personal information is recorded and managed within corporate information systems whose existence is publicly accounted for and for which there is an accountable manager (no secret or hidden information systems or personal caches of information about individuals);
   - use of appropriate managerial and technical controls to protect the confidentiality and integrity of personal information;
   - ensuring that retention and disposal authorities are in place for all data in all personal information systems, including special conditions for research and statistical data and corporate memory and archival data which will be kept for much longer periods than normal data. For long-term data retention, the identifiable information should be used only for one of the permissible purposes set out in the *FOIPP Act* and, if it is retained for research or statistical purposes, identifiable personal information should not be used for purposes to make a decision that directly affects the individual involved. In other words, sets of identifiable research or statistical personal data should not be re-activated for administrative decision making directly involving an individual unless the individual has consented to the new use of that personal information.

   These various information integrity, security and management factors are discussed in more detail in Part 6 of this study.

In addition, the *FOIPP Act* establishes a right of individuals to access and to correct or annotate (i.e., place a disclaimer on the record or flag the data) of the information held about them. It also establishes an independent review mechanism through the Information and Privacy Commissioner to resolve complaints from individuals about access to, correction of and the handling of their personal information and for investigating how organizations are meeting the privacy protection requirements of Part 2 of the legislation.

Where the Information and Privacy Commissioner has reason to believe that a program or system (for example, application of smart card technology) is adversely affecting the protection of privacy (or may do so in the future), the Commissioner may investigate or audit the program or system.

## IMPLEMENTING PRIVACY PROTECTION FOR INFORMATION SYSTEMS

As indicated above, Part 2 of the *FOIPP Act* establishes controls over personal information in order to protect individual privacy. These fair information practices are largely based on a special life-cycle approach to the management of personal information.

This forms a sub-set of the life cycle for information management that underpins both technology management and modern electronic record-keeping. It requires that privacy issues relating to the collection and compilation, completeness and accuracy, protection, use, disclosure and retention of personal information be integrated into the systems development and implementation processes of an organization.

**Strategy**

Develop corporate privacy protection policies and procedures that enable you to:

- establish a methodology for addressing privacy protection and related security issues in planning and establishing functional specifications for new or modified personal information systems;
- review personal information systems and bring them into compliance with Part 2 of the *FOIPP Act*;
- review forms used in the collection of personal information to ensure that they meet the collection and notification requirements of the *FOIPP Act*;
- establish a security policy which includes protection of privacy as one of its aspects; and
- identify and manage the data matching of personal information.

## PLANNING NEW AND MODIFIED PERSONAL INFORMATION SYSTEMS

The privacy protection requirements set out in Part 2 of the *FOIPP Act* should be fully integrated into the design, construction and implementation of computerized information systems used to process personal information.

School jurisdictions must collect, create and use a wide variety of personal information in order to carry out their programs and deliver their services. Increasingly, computer and computer-related technology are being used to provide faster, easier and more cost-effective ways of handling and storing this information. Personal computers and laptops are becoming part of the essential equipment of officials, employees and teachers.

In addition, computers have become an important aspect of the classroom. Students are trained on and permitted to use sophisticated software and network applications as part of the education process. This often permits them to reach out far beyond the school walls to access information not previously available to them and to interact with people around the world. It also permits them to actively carry on school-based activities from home and at any time.

This has the definite advantage for school jurisdictions of helping to streamline processes and enhance education programs. Indeed, administrators strongly encourage greater automation and integration of information and operational systems as a vital part of "re-inventing" the education system.

At the same time, these applications of new technology make individuals nervous about their privacy being threatened and their personal information being put to uses that they never intended when it was given to the public body. Surveillance is easier and can be done in a more surreptitious and pervasive way. Public bodies, including schools, have traditionally enjoyed high public confidence in how they collect, use and protect personal information.

To ensure that privacy protection considerations, as set out in Part 2 of the *FOIPP Act*, are taken into account in the application of new technologies, the Information and Privacy Commissioner frequently asks all public bodies to undertake a privacy impact assessment for major projects involving the large and/or innovative application of information technology.

The challenge for school jurisdictions is to integrate privacy protection into technology systems development in ways that enhance information and data quality, integrity, accuracy and confidentiality. Privacy and security measures should not be viewed as immovable barriers to applying innovative technology but rather as essential components of modern systems that serve to build public confidence in the use of technology to promote more effective and efficient public administration.

Quality management of technology should go hand in hand with privacy protection.

***Strategy***

Establish practices and procedures which provide for the consideration of the requirements of Part 2 of the *FOIPP Act* in the planning, design, development of specifications and implementation of information technology to new or modified information systems used to collect, compile, process, store, use, disclose or manipulate personal information.

***Strategy***

Require that a privacy impact assessment (PIA) forms part of the authorization for all information systems used to collect, compile, process, store, use, disclose or manipulate personal information. This document should be the basis for attesting to the superintendent that measures have been integrated into the information system to meet the requirements of Part 2 of the *FOIPP Act*. (A model form is provided in Chart 3.)

# CHART 3
# MANAGEMENT TOOL FOR UNDERTAKING PRIVACY IMPACT ASSESSMENTS FOR NEW INFORMATION SYSTEMS

## PRIVACY IMPACT ASSESSMENT

### 1. Introduction:

Provide:

- name of system;
- a high-level overview of the system, its purposes and business objectives;
- a summary of the privacy impact assessment—privacy issues involved, assessment of approaches for addressing these issues in systems development and recommendations regarding systems development; and
- name of contact accountable for the system.

### 2. Collection Requirements

- Identify the authority (statutory, law enforcement or program) under which the system is being established.
- State the purpose(s) of the collection of personal information.
- Provide a complete summary of the data elements to be collected and demonstrate that these are limited to those directly related to and necessary for the program or activity supported by the information system.
- Show authority under Section 33(2) of the *FOIPP Act* for any collection of personal information that will not be acquired directly from the individual the information is about.
- Discuss procedures for notifying individuals about the authority, purposes and official accountable for the collection under Section 33(2) of the *FOIPP Act.*

### 3. Accuracy

Describe the procedures, including information system features, which will be used to ensure, in a reasonable and practical manner, the accuracy of the personal information collected.

### 4. Retention

Describe the procedures and features within the system which ensure that personal information (data) used to make a decision directly affecting an individual will be retained for a minimum period of one year.

### 5. Use/Disclosure

- Describe all the intended uses for the personal information held on the system and connect these to the purposes of the program or activity the system is supporting (Section 37 of the *FOIPP Act*).
- Describe all accepted disclosures of personal information from the system and their authorization under Section 38 of the *FOIPP Act.*
- Provide generic user profiles indicating ability to access, use, change, delete, copy, print and communicate identifiable personal data in the system.
- Describe the generic measures to be included in the systems design to meet these controls on use and disclosure of specific identifiable personal data elements.

### 6. Data Matching and Linkage

- Identify all data matching and linkage that is proposed to be done with personal information held on the system.
- Provide authority for each data match or linkage through reference to specific sections of Part 2 of the *FOIPP Act.*
- Describe the process that will be followed to judge feasibility and obtain approval for each data matching and linkage application.

7. **Security**

Provide a security assessment with a general overview of the measures that will be taken to address the applicable common threats to electronic information systems, namely:

- unauthorized access to and use of the system;
- threats to the availability and integrity of the data;
- risk of theft or unauthorized destruction of information or data;
- interception of information or systems operating protocols during communication of data;
- careless or hostile employee acts; and
- natural or other disaster.

8. **Information Management**

Describe any information management approaches and procedures that are being put in place to ensure proper management of both the paper and electronic files associated with the system, and name the official who is accountable for the management of the system from both the information and privacy perspectives.

9. **Privacy Impact Analysis**

Discuss and analyze potential impacts on privacy, and exposures and how may they be addressed:

- Would the activities supported by the system be commonly seen as privacy intrusive?
- Would the activities result in privacy-intrusive behaviour?
- Do the applications in the system require collection of personal information?
- Do the applications require the use of personal information already collected or compiled for other purposes, and how are these justified under Part 2 of the *FOIPP Act*?
- Basically, how will personal information be protected and held secure?
- What are the generic uses and disclosures envisioned through the system and who will be undertaking these?

Describe the technology and discuss how it can impact on privacy protection, both negatively and to enhance privacy protection.

Discuss the options available for addressing privacy issues, and make a recommendation about how the school jurisdiction should proceed.

**Signature:** Official responsible for the information system.

**Acceptance:** Superintendent or delegated responsible senior official.

**Comments:** Comments and/or directions from officer accepting privacy impact assessment.

## PRIVACY IMPACT ASSESSMENT

A privacy impact assessment (PIA) is simply a systematic approach to assessing the legal requirements of Part 2 of the *FOIPP Act*. The approach is important for school jurisdictions because they hold a great deal of relatively sensitive personal information. Public confidence is related, in part, to an organization's ability to protect such information. At the same time, it is important that privacy protection not become a major barrier to accomplishing the core goal of providing quality educational services. The PIA can serve as a tool for ensuring that reasonable and adequate measures are taken to protect the privacy of individuals whose information is processed and available on a personal information system while adapting such measures to the milieu and business needs of the educational organization.

A PIA is best carried out during the systems design process. It should involve joint analysis by the FOIPP co-ordinator, the information technology representative and the program area for which the system is being developed.

Briefly, a PIA should include

- a systems overview;
- an authority statement;
- a description of the types of personal information involved and the level of sensitivity;
- an analysis of privacy issues relating to collection, accuracy, retention, use and disclosure of the personal information and how these will be met in the system;
- an assessment of security measures needed to protect the personal information;
- an overall assessment of the privacy impact and a recommendation as to what should be included in the design specifications to meet the requirements of Part 2 of the *FOIPP Act*; and
- a sign-off by the program, information technology and FOIPP managers, as well as by the superintendent.

If the technology and related privacy issues are significant or the technology relatively innovative, then the school jurisdiction may wish to seek advice on the project from the Office of the Information and Privacy Commissioner. An example of the first situation might be a proposal to connect a series of personal data sources that have not been previously connected electronically. The second situation might occur if it were proposed to issue smart cards holding personal information.

A PIA also should include:

1. *Application description:* Describe the proposed technology application being applied to the management of personal information within the program or activity. Particular mention should be made of the privacy implications of the application, both positive and negative. For example, a smart card may permit access to a wide range of personal information about an individual that is otherwise not available. However, the card also may permit segmentation and encryption of such data in ways that protect the privacy of the individual in a far better manner than any other method of administering the program or activity.

   There should be a systems overview that describes the technology and its purposes and benefits in plain, non-technological language.

2. *Authority for collection:* There should be a concise statement of the statutory, regulatory or program/activity authority for collecting the personal information as required by Section 32 of the *FOIPP Act*.

3. *Nature of the personal information:* What personal information data elements will be collected and how are these related directly to and necessary for the program or activity? These limits on collection are required by Section 32 of the *FOIPP Act*.

4. *Purpose(s) of collection:* Identify the purposes of the collection. Describe why it is necessary to collect this personal data and how it is related to the authority to collect the information.

5. *Method of collection:* Describe how the personal information will be collected and, if it is to be linked to existing information, the authority the system will rely upon for doing this. If the personal information is to be collected indirectly (i.e., from a source other than the individual to whom it relates), then the authority under Section 33(1) of the *FOIPP Act* for the collection must be cited.

6. *Notification:* Where personal information will be collected directly from the individual to whom it relates, show how the system will provide notification of the authority, purposes and accountability for the collection as required by Section 33(2) of the *FOIPP Act.*

7. *Accuracy of the information*: Basic technical details should be provided to show how the system will function in ensuring the accuracy and currency of personal information used for decision making directly related to the individual.

8. *Use:* Describe the uses that will be made of the personal information and the basic generic structure for governing such use on a "need-to-know" basis, as required by Section 38(g) of the *FOIPP Act.* This should include an analysis of authorities to read, change, delete, copy, print and communicate the various data fields relating to the personal information, which then will govern the implementation of the system. As well, the description should deal with what audit features will be put in place to monitor use and disclosure of the personal information. This is important because an authorized user may still gain access to and use or disclose personal information for non-authorized purposes.

   Chart 4 presents a limited example of a data field checklist for a fictional student registration system accessed by authenticated password or token.

### CHART 4
### DATA FIELD CHECKLIST

| Data Field | Accessed By | Read Only | Add Data | Change Data | Delete Data | Copy Data | Print Data | Commun-icate Data |
|---|---|---|---|---|---|---|---|---|
| Course Name | Student | Y | N | N | N | N | Y | N |
| | Parent | Y | N | N | N | N | Y | N |
| | Teacher | | Y | Y | N | Y | Y | N |
| | School Adminis-trator | | Y | Y | Y | Y | Y | Y |

9. *Controls on disclosure:* There should be a description of all disclosures of personal information within the system that the school jurisdiction will make on a regular basis. This should identify all external organizations that will be given access to the personal information, the extent of the disclosure (for example, identifiable data, summary data or non-identifiable data) and the basis under Section 38 for making the disclosure. For identifiable personal information, a paragraph in Section 38 of the *FOIPP Act* must apply before disclosure can be made. The statutory or

business reason for each type of disclosure should be given, along with any special privacy or security conditions under which it is made.

10. *Data matching and linkage:* Describe any data matching or data linkage programs between the new system and other information systems and how these meet the use and disclosure provisions of the *FOIPP Act.* Data matching requirements are discussed in more detail later in this part of the study.

11. *Security measures:* Provide a security assessment and describe the security measures that will be implemented to ensure the integrity of the personal information and to prevent its unauthorized access, collection, use, disclosure or destruction, as required by Section 38 of the *FOIPP Act.* A more detailed technical discussion of security issues appears in Part 6 of this study.

12. *Information management:* Describe the information management approaches and procedures that are being put in place to ensure proper management of both the paper and electronic files associated with the system, and name the official who is accountable for the management of the system from both the information and privacy perspectives.

13. *Privacy impact analysis:* Provide an overall analysis of the privacy issues involved with the information system and the options and recommended approaches which are being put in place to address these from the combined perspectives of business need, privacy duties and obligations and quality application of technology. The overall goal should be to integrate privacy requirements into the business and technology goals of the school jurisdiction.

## SECURITY OF PERSONAL INFORMATION

Section 36 of the *FOIPP Act* requires a school jurisdiction to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

*Reasonable security arrangements* are usually practices and procedures expressed through a security policy approved for use within an organization. This policy should deal with physical, personnel and information technology security and be geared to a risk and threat analysis of the information and assets in the custody or under the control of the organization.

Security of personal information systems involves a separate detailed security assessment, as part of the overall PIA. This should be a detailed technical review by someone with expertise in information technology security but the suggestions and recommendations for the security measures to be required in the specifications for the information system should be provided in the PIA report.

A security assessment should include:

- a statement of the sensitivity of the personal information involved, drawn from the PIA;

- a statement of business lines being developed, a description of their content (for example, administration of a benefit program) and an initial assessment of expected standards for information and data integrity, quality, accuracy, availability and confidentiality;
- the location and distribution of the information (for example, central office, local area offices, mainframe or distributed network, all electronic or combination of electronic, hard copy and other formats, etc.);
- potential threats (physical and technical, accidental and deliberate), to the personal information balanced against the likelihood of occurrence and the consequences that could result;
- an appraisal of the various risks based on the above; and
- general recommendations for a security approach.

More details on analysis of security measures are provided in Part 6 of this study.

## CONTRACTING

When the development and/or operation of personal information systems is contracted out, the need to develop privacy impact and security assessments should be among the privacy requirements pertaining to Part 2 of the *FOIPP Act* included in any management or operations contract governing the project.

### PROCESS FOR A PRIVACY IMPACT ASSESSMENT

In order to integrate privacy and related security considerations into the design, construction and implementation of new computer information systems that are used to process personal information, school jurisdictions should follow the general process outlined in Chart 5.

## CHART 5
## PRIVACY IMPACT AND SECURITY ASSESSMENT

| ✓ | Steps | Considerations |
|---|---|---|
| **Privacy Impact and Security Assessment** | | |
| | Analysis of new systems development and/or improvement in order to achieve FOIPP compliance | • Involve senior personnel, the FOIPP co-ordinator and senior records officers along with information technology (IT) and IT security people in the planning phases. |
| | Issues to be discussed | • Privacy rights of individuals<br>• Protection of personal information<br>- management of information<br>- collection or compilation of data<br>- controls on accuracy<br>- use and disclosure<br>- protection (security)<br>- disposal<br>• Reflect legal and policy requirements |
| | Develop | • Privacy impact assessment<br>• Security impact assessment<br>• Forms<br>• Technical specifications<br>• FOIPP specifications |
| | Information and Privacy Commissioner's Office | • Send the business analysis, technical and FOIPP specifications along with the planned privacy and security impact assessment to the Information and Privacy Commissioner's (IPC's) Office for comment. Ask for 30-day turnaround.<br>• As the project progresses, continue to keep the IPC's Office up to date. |
| | Communications | • Announce privacy and security impact study and provide details to public.<br>• On opening of the database for employee or public usage, notify everyone of the security features. |
| | Develop | • Continue development but now incorporate suggestions from IPC's Office. |
| | Cost/Benefit Analysis | • Build the cost of privacy and security into the plan. |

### Privacy Impact Assessment

The privacy impact assessment should contain the following information:

- nature and sensitivity of the personal information involved
- potential privacy principles and issues arising from the project and how they should be addressed
- purposes of personal information and authorized disclosure procedures
- how FOIPP compliance will be met in conceptual solutions
- assessment of privacy impact as high, medium or low
- general recommendations for potential solutions

### Security Impact Assessment

The security impact assessment should include:

- a statement on sensitivity of personal information taken from the privacy impact assessment
- a statement on business lines being developed, description and an initial assessment of expected standards for information and data integrity, quality, accuracy, availability and confidentiality
- location and distribution of the information
- potential threats
- an appraisal of various risks based on the above
- general recommendations for a security approach

### Contracting

When the development of personal information systems is contracted out, the need to develop privacy impact and security assessments should be among the privacy requirements pertaining to Part 2 of the *FOIPP Act* included in any management or operations contract governing the project.

## REVIEW OF EXISTING PERSONAL INFORMATION SYSTEMS

The collection, use, disclosure and retention requirements of Part 2, Protection of Privacy, in the *FOIPP Act* are very much oriented to information management practices. These new requirements will require modifications to the information management practices of most public bodies and to the operation of manual, automated and electronic information systems that are used to collect, compile, organize, manipulate and retrieve personal information.

***Strategy***

Establish policies and organizational structures that will facilitate the integration of privacy protection requirements and practices into the ongoing management of personal information systems and plan how to bring existing program activities and personal information systems into compliance with Part 2 of the *FOIPP Act*.

This will involve a review of existing information systems used to collect or compile, process, use, disclose, store or manipulate personal information. Since this may be a large task, remedial measures should be planned and implemented over a reasonable number of years.

In bringing information systems into compliance with the privacy provisions of the *FOIPP Act*, school jurisdictions will:

- support the right of students, parents and the general public to know what personal information schools collect and how this information is used;
- support the right of individuals to access their own personal information;
- help assure individuals that their personal information is protected from unauthorized collection, use or disclosure;
- ensure public confidence in such systems and the programs which they support in regard to how personal information is handled;
- contribute to the highest quality of management and effectiveness for such systems, especially automated or electronic systems; and
- establish additional accountability for the protection of individuals' right of privacy by improving the management of personal information.

## CHART 6
## FOIPP CHECKLIST FOR THE REVIEW OF PERSONAL INFORMATION SYSTEMS

| Reason | Mandatory | Optional |
|---|---|---|
| | **Collection of Personal Information (Sections 32 and 33)** | |
| Authorization for Collection (Section 32) | What is the authorization for collection of personal information in the system?<br>• authorized by or under an Act of Alberta or Canada;<br>• purposes of law enforcement; or<br>• relates directly to and is necessary for an operating program or activity of the public body.<br>At least one response must be *yes*. If none of the above statements elicits a *yes* response, a review of the collection is required to determine if it is still needed by the public body and, if so, how it may be brought into compliance with the *FOIPP Act*. | Is there a collection control and approval mechanism in place to ensure that the minimum amount of personal information necessary to carry out a program or activity is collected? If the answer is *no*, consideration should be given to establishing such a control and approval mechanism. |
| Manner of Collection (Section 33[1]) | Is the personal information in the system collected directly from the individual the information is about (direct collection)?<br>If the answer is *yes*, see Notification of Collection below.<br>If the personal information in the system is collected from a source *other than the individual the information is about* (indirect collection), what is the authority in Section 33(1)(a) to (k) for indirect collection and is evidence of this authority provided in the documentation for the system?<br>If the answer to the last question is *yes*, a revision of procedures or of the collection itself may be required, such as commencing to collect the information directly from the individual, seeking his or her consent for an indirect collection of the information or ceasing the collection. | |

| | | |
|---|---|---|
| Notification of Collection (Section 33[2]) | Is notification of the following points provided to the person from whom the information is collected?<br>• The specific purposes for which the information will be used;<br>• The specific legal authority for the collection of information; and<br>• The title, address and telephone number of an official in the public body who can answer questions about the collection of personal information.<br>Determine the method of notification (e.g., notice on form, pamphlet, oral notice, pop-up screen on computer terminal, etc.) and the completeness of the notice against the requirements of the *Act*.<br>The answer must be *yes* to all relevant points and procedures in place or modifications to the processes of notification may be needed.<br>If notification as described above is *not given* to the person from whom the information is collected, does one of the following conditions exist?<br>• Does one of the paragraphs in Section 33(1)(a) to (k) apply? Or<br>• Has the head of a public body excused the need for notification because compliance would result in the collection of inaccurate information?<br>If neither of these questions can be answered with a *yes*, a revision of collection procedures or the type of information collected is required. | If personal information in the system is collected from a *source other than the person the information is about* (indirect collection):<br>• Is notification of collection provided to the person the information is about?<br>• In cases where personal information is downloaded from another public body's system rather than input directly, is the individual the information is about informed of this data sharing when the other public body collects the information?<br>If the information is either collected on an electronic form or keyed directly into the database during an interview:<br>• Is there provision for obtaining the individual's signature authorizing collection and use of the information?<br>• Is a hard copy of the completed form or a printout from the database provided to the person from whom the information is collected?<br>• Is a hard copy notification of collection provided to the person from whom the information is collected?<br>• Does the office retain a copy of the authorization or notification?<br>If the answer to any of the above questions is *no*, is some other form of audit trail maintained of the authorization for collection, the source of the information and the notification of collection and use? |

<table>
<tr><th colspan="3">Accuracy of Information (Sections 34[a] and 35)</th></tr>
<tr><td></td><td>Does the system meet the following requirements?<br>• Can it be determined when the record containing personal information was last updated?<br>• Is a record kept of the source on which the change was based, either through a hard copy or an automatic logging of transactions so that it is possible to re-create any addition, deletion or modification of information?<br>• Are procedures in place to ensure that individuals can review their own personal information and request correction or annotation in case of error or omissions?<br>• Are procedures in place to send a notification of a correction or annotation of personal information to any other public body or third party to which the information has been disclosed during a one-year period prior to the correction or annotation?<br>• Is a record kept of all updates to files, including requests for correction or annotation?<br>• Is there a system of verification for personal information collected and for its entry on the system?<br>• Are recovery routines and procedures in place and are they designed to minimize the possibility of misrouting interrupted output?<br>• Where changes of processing state are required, are procedures documented and implemented to ensure the integrity of the operating system and supporting software?<br>• In electronic systems, are computerized records compared at appropriate intervals to an independent source as a basis for verifying the accuracy and completeness of stored data?<br>• Are there adequate procedures to automatically identify and correct errors and omissions?<br>• Does a responsible authority review these actions and procedures?<br>• If the response to the above questions is generally <i>no,</i> then a revision to system procedures is required.</td><td></td></tr>
<tr><th colspan="3">Retention of Personal Information (Section 34[b])</th></tr>
<tr><td></td><td>If information has been used to make a decision that directly affects an individual, are procedures in place to ensure that the information is retained for at least one year after use?</td><td>Are procedures in place for disposition of personal information and are actual records schedules agreed to and signed for all information in personal information banks in the custody or under the control of the public body?<br><br>If the response to either question is <i>no</i>, the public body needs to establish a records scheduling process or to make a revision in current records scheduling procedures and practices.</td></tr>
</table>

## Protection (Section 36)

Does the system meet the following requirements, as appropriate to the sensitivity of the information on it?

- Are all personal information sources identified?
- Do a security policy and security procedures govern operations?
- Is there a responsible official who has the security authority for the system?
- Are there documented procedures for collecting, processing, accessing, transmitting, storing and disposing of personal information?
- Do security procedures cover personnel, physical and information technology security, including:
  - a threat-and-risk management methodology;
  - a process for designating sensitive information and assets and issuing sensitivity statements for electronic systems;
  - a system of authorization and access procedures such as the issuance of identification cards and the maintenance of control records for gaining access to sensitive personal information and sensitive material and items such as keys, codes, combinations, badges and system passwords;
  - controls over authorization to add, change and delete personal information on a system and transaction controls to determine when personal information on a system was last updated, who updated it and who has accessed it;
  - procedures to ensure that competent personnel are involved with the maintenance of electronic systems in order to ensure configuration control of equipment, systems, networks and the updating of operating procedures;
  - procedures for ensuring communications security and appropriate controls over cryptographic materials where this is required;
  - procedures for adequate reference checks and screening of personnel commensurate with the sensitivity of the personal information involved and access controls that restrict access to personal information for the purposes for which the information has been collected and used and to those officials and employees who have a "need to know" the information (i.e., access is limited to the specific portions of the personal information needed for the function being performed); and
  - appropriate physical security measures such as security access zones, locked rooms, storage cabinets, and controlled positioning and access to computer terminals and faxes to prevent random access, checkout and secure transmission procedures for files, and secure disposal procedures for records and equipment commensurate with the sensitivity of the personal information and its vulnerability to compromise.

Is there any monitoring and review of the general effectiveness of security measures, including those relating to the protection of personal information?

If the general response to the relevant requirements is *no*, it may be necessary to establish security policies and procedures for the personal information system or to revise them.

|  |  |  |
|---|---|---|
| **Use (Section 37)** |  |  |
|  | Is the personal information in the system used only for the purpose for which it was collected or for a use consistent with that purpose?<br>If not, is the use one to which the individuals have consented in the prescribed manner?<br>If not, is the use for a purpose for which information may be disclosed under Sections 38, 40 or 41 of the *Act*?<br>If one of these questions is not answered with a *yes,* then the uses of the personal information in the system need to be examined and activities that do not meet the above tests stopped. |  |
| **Disclosure (Section 38)** |  |  |
|  | Is there disclosure of information from the system? That is, is any person or body outside the organizational unit that operates and uses the system allowed access (to information on or in the system) either directly through electronic means or through receipt of hard copy, tapes, diskettes or other copies? Does the disclosure fall within one of the provisions of Sections 38(a) to (bb) of the *Act*? | If the answer is *no*, then the disclosures must be reviewed and those which do not meet the categories in Sections 38(a) to (bb) stopped. |
| **Research or Statistical Purposes (Section 40)** |  |  |
|  | In the case of disclosure for research or statistical purposes, the following conditions *all* must be met for a research project to be in compliance with Part 2 of the *Act*:<br>• The purpose of the research can not reasonably be accomplished without access to the information in individually identifiable form or the Information and Privacy Commissioner has approved the disclosure;<br>• Any record linkage is not harmful to the individuals the information is about;<br>• The benefits of the record linkage are clearly in the public interest;<br>• The researcher has signed an agreement to comply with security and confidentiality conditions, to meet a schedule of the destruction of individual identifiers and to ensure that there is no subsequent use or disclosure of the information in individually identifiable form without express authorization; and<br>• The agreement meets the standards set out in the *FOIPP Regulation.*<br>Conditions must be in place to ensure that all research conducted with identifiable personal information from a personal information system meets these criteria and that the use and disclosure of such information is carefully monitored to ensure that all conditions are being met. |  |

| Data Matching | | |
|---|---|---|
| | If there is data matching occurring which involves information from the system:<br>• Do the uses involved in the matching meet the requirements of Section 37? And/or<br>• Do any disclosures made for matching purposes meet one of the conditions in Section 38?<br>If data matching is occurring:<br>• Are the matches of information for a non-administrative purpose that has no direct affect on the individuals concerned?<br>• Are the matches of two or more databases of information collected and held for the same purpose? (The exclusion is implicit in the definition of data matching.)<br>• Do the matches involve programs which review the contents of a record system to remove or correct items where there is no intention to take administrative action?<br>• Do the matches involve programs which co-locate items previously in separate locations (provided the purposes for which the information collected or compiled continue to apply)?<br>• Do the matches involve research, statistical or program evaluation purposes where the output is in a non-identifiable form?<br>• Are the matches authorized through a permissible disclosure set out in Section 38(a) to (bb)?<br>If the answer is *no* to either of the above, the system can not be considered to be in compliance with Part 2 of the *FOIPP Act*. | Is there notification of the individuals whose personal information may be the subject of data matching at the time the information is collected? |

The checklist can apply to both electronic and other automated and manual information systems.

## DATA MATCHING

Data matching is defined as the comparison of personal data obtained from different sources, including both electronic and paper-based formats, for the purpose of making decisions about individuals to whom the data pertains. Data matching is therefore an activity involving the collection, use and disclosure of personal information. Included in the definition of data matching is data linkage, also known as data profiling.

Data matching plays a valuable role in increasing the efficiency of a wide variety of government programs. For example, school jurisdictions might be asked to share personal data with provincial or municipal public bodies to determine if certain individuals or families should qualify for or continue to receive certain income support or social benefits. As well, it may be useful for a single school jurisdiction or several jurisdictions to profile developing student populations using several diverse data sources and to use these profiles to determine which students should qualify for particular programs. Because they rely on the comparison or merging of diverse sources of personal data, data matching and profiling also can have a major impact on the privacy of individuals.

For this reason, there is a need to balance the requirements for efficiency and effectiveness in programs with the potentially invasive nature of the activity. As well, there needs to be careful attention to the quality of the data being matched and its reliability for pursuing administrative actions against individuals.

There are no specific controls over data matching or linkage in Part 2 of the *FOIPP Act.* However, the collection, use and disclosure provisions govern how such activities can be carried out.

**Strategy**

Require that all data matching activities involving personal information be reviewed by the jurisdiction's FOIPP co-ordinator and, where appropriate, that advice be sought from the Office of the Information and Privacy Commissioner.

When carrying out matching activities, school jurisdictions should:

- determine whether the match is permitted by the use and disclosure provisions of the *FOIPP Act*;
- prior to initiating a matching program (but not each individual matching activity), assess the feasibility of the proposed match, including the potential impact on the privacy of individuals and the costs and benefits of the data matching program;
- notify the Information and Privacy Commissioner of a new matching program by providing that Office with a copy of the jurisdiction's assessment at least sixty days before it is to commence;
- approve data matching programs at a senior level authorized by the head of the school jurisdiction to make such decisions;
- ensure that all matching activities are accounted for in relevant personal information bank descriptions; and
- subject information generated by a matching program to verification with original or additional authoritative sources before that information is used for an administrative purpose.

These provisions do not need to be applied to matching or linkage:

- involving information that has been rendered anonymous or is identifiable but the purpose of the data matching or profiling is not to make any decisions that would directly affect the individuals involved;
- involving two or more databases of information collected and held for the same purpose;
- involving programs which review the contents of a record system to remove or correct items where there is no intention to take administrative action;
- involving programs which co-locate items previously in separate locations, provided the purposes for which the information collected or compiled continue to apply; or

- involving research, statistical or program evaluation purposes where the output is in non-identifiable form.

A school jurisdiction may become involved in a data matching activity because it wishes to use this technique in its administrative or operational processes. In this case, it is called the *matching public body*. There are a number of steps that a matching public body should undertake when deciding whether or not to establish a data matching program.

Alternatively, a school jurisdiction may be asked to disclose personal information for data matching purposes in another organization (sometimes another public body, but not necessarily). In such instances, the school jurisdiction is known as the matching source.

In both instances, most of the responsibilities of matching public bodies and matching sources involve deciding if data matching can be carried out within the statutory provisions of Part 2 of the *FOIPP Act*.

### *Basic Questions*

In considering the implementation of the privacy protection requirements in Part 2 of the *FOIPP Act* for electronic information systems which store, manage, manipulate or communicate personal information, the following questions are pertinent.

❑ Is there a process in place to ensure that a PIA is conducted during the development of new and modified information systems?

❑ When a PIA is conducted, are we satisfied with the measures recommended to ensure the system meets the legal requirements of Part 2 of the *FOIPP Act*?

❑ Is this technology project of such a significant and/or innovative nature that it merits consultation with the Information and Privacy Commissioner?

❑ Is a process and reasonable schedule in place to undertake the review of existing information systems dealing with personal information and any related forms to ensure that each system is brought into compliance with the requirements of Part 2 of the *FOIPP Act*?

❑ Are all program areas and schools identifying all data matching referred to the FOIPP co-ordinator for review and approval?

# PART 6: FOIPP AND INFORMATION MANAGEMENT

## MANAGING ELECTRONIC RECORDS

Sound information and records management is essential to the effective administration of FOIPP. The *FOIPP Act* puts a much greater emphasis on the control of document-based information systems, electronic and paper. This is essential where electronic information systems are increasingly used to create, obtain and distribute the records of the organization.

School jurisdictions should be undertaking management of records and information for reasons that are significantly broader than the requirements of the *FOIPP Act*. Organizations create, maintain and manage recorded information to provide tangible evidence of business activities and transactions. Generally, information and records management is undertaken to:

- support policy formation and managerial decision making;
- improve client services and support better performance of business activities;
- support consistency, continuity and productivity in operations, administration and management;
- protect the interests of the organization and the rights of clients, the public and employees;
- provide protection and support in litigation, including the better management of risks associated with the existence or lack of evidence of activities or events;
- facilitate research and development activities; and
- enable the organization to meet legislative and regulatory requirements.

The creation, obtaining and dissemination of records through the use of information technology has two perspectives, one for internal use (LAN or WAN applications) and the other for public access to information provided by the school jurisdiction via dial-up modem or other methods such as the Internet or an intranet or extranet.

Whatever the broader information implications, the provisions of the *FOIPP Act* have a major impact on the management of information and records in school jurisdictions, particularly electronic records.

## FREEDOM OF INFORMATION

The access rights to the records provided in the *FOIPP Act* are intended to make public bodies more open and accountable to the public. Inadequate record-keeping can contribute to, or even be instrumental in, failures of appropriate accountability to students, parents and the general public. In the case of FOIPP requests for access, this places a school jurisdiction in default of the *FOIPP Act*. This may lead to:

- challenges to its credibility and reputation in carrying out its mission and role; and

- the school jurisdiction's being exposed as negligent or ineffective in its responsibilities through orders and reports of the Information and Privacy Commissioner and commentary from applicants and interested members of the public.

Some common issues are outlined below.

1. *Ability to find records:* The access provisions of the *FOIPP Act* assume an ability on the part of public bodies to identify, locate and produce records in response to requests. Such ability is crucial both in making information routinely available to the public and in responding to FOIPP requests.

   The failure to capture records in effective record-keeping systems is the most commonly cited problem associated with inadequate management of information and records. This results in difficult and time-consuming searches for records and uncertainty that all records relevant to a FOIPP request have indeed been located. This is particularly an issue when no records can be found in relation to a subject on which it appears a school jurisdiction should have created and maintained records.

   Applicants frequently challenge the adequacy of a search for records by a public body. Demonstrating the adequacy of a search is much more difficult if there are no established record-keeping systems that can be shown to have been searched in a systematic and reasonable manner.

2. *Standard of documentation*: A school jurisdiction should have a standard of documentation. This involves a clear policy direction from senior management as to when it is expected that officials and employees will document the business activities and transactions of the organization.

   Employees must understand and be held accountable for documenting their activities or transactions. As well, there is a need in the modern electronic work environment to establish information technology systems that create and maintain appropriate information that can be viewed as the authoritative version with the context and integrity to document an activity or transaction.

   In some instances, records are created but they are inadequate from an accountability perspective because they are not full and accurate or it is impossible to determine the authoritative version on which a decision or other action was based.

   There also is a need for clear direction on what records may be deemed to be transitory. This issue has come up most prominently in FOIPP requests dealing with records which involve, in part, the new technologies of electronic messaging (e-mail) and voice mail.

   Finally, there is a need for standards of documentation to clearly indicate that records created in documenting the activities or transactions may not be altered or destroyed without written approval of senior management. This emerges as an issue in office systems that are now designed to easily manipulate and reuse information in a variety of records. There is a need to be able to determine which versions of documents were used at particular times (version control) and to capture the actual documents used to support a decision, action or transaction. Alteration or destruction of records can be a very serious matter, especially if it is done to evade a FOIPP request. Such action could lead to disciplinary action. This was the case in the Department of National Defence in regard to the Somalia inquiry.

3. *Controls over disposal:* Cost-effective business practices dictate that a school jurisdiction have a systematic process for disposing of records, including those in electronic form, as they become inactive and are no longer needed for business purposes or the long-term operations of the organization; for example, to protect the organization's interest in litigation.

   This process, known as records scheduling, has several advantages from a FOIPP perspective. It provides control over records disposition, including transitory records, so that organizations know what was destroyed and when. As a result, organizations do not search for records that no longer exist. It also provides an official approval process for the disposition of records based on business needs that can be referred to when an applicant requests records that have been disposed of by the organization. Finally, it moves records through the system, thus reducing the exposure of the school jurisdiction to requests for older records, which may be very labour intensive to deal with.

Older records needed to record activities and protect individuals' interests and to provide a long-term corporate memory for a school jurisdiction, can be placed in the Provincial Archives of Alberta or the official archives of the jurisdiction. FOIPP requests may then be dealt with under the auspices of the archival body. Such bodies are usually better able to take the time needed to deal with older records.

In summary, lack of a systematic scheduling system for records can mean that:

- older records are retained far longer than needed;
- there is random destruction of records, which can be embarrassing for an organization or may even expose it to risks of litigation;
- there is no official authority for the legitimate disposal of records that are of no further use, including transitory records; and
- resources may be wasted looking for records that no longer exist.

4. *Ability to routinely disclose records outside the FOIPP Act:* A public body needs:

   - to have effective control over the records and information it creates and collects; and
   - to be knowledgeable of such records and information.

This control and knowledge is required to make effective decisions about which records should either be released on a routine basis or actively disseminated to the public. This is an essential practice in support of more openness in public administration and in avoiding large numbers of FOIPP requests, which are extremely time-consuming to process.

## PROTECTION OF PRIVACY

As indicated in Part 4, the *FOIPP Act* establishes controls over personal information in order to protect individual privacy. These are generally called *fair information practices* and are largely based on a special life-cycle approach to the management of personal information.

These practices form a sub-set of the life-cycle for the management of recorded information that is required in modern record-keeping and cover the collection and compilation, completeness and accuracy, protection, use, disclosure and retention of personal information.

Effective implementation of the privacy protection measures set out in Part 2 of the *FOIPP Act* requires adoption of the management practices for personal information. These practices are dealt with in detail in Part 3 of this study.

***Strategy***

Ensure that the management of all recorded information in your organization, including electronic information, is governed by a corporate information management policy. This should be developed with the administration of FOIPP in mind and include appropriate references to FOIPP requirements in both the policy statements and the procedures, practices and standards used to implement the policy.

The program for information management of recorded information should be anchored in a number of policy objectives and statements that guide its operation within the public body. FOIPP encompasses all the recorded information in the custody or under the control of a public body. Thus, the principles underpinning the management of recorded information should:

1. *Apply to all records* as defined in the *FOIPP Act*, including personal information and electronic records.

2. *Be based on the management of information as a corporate resource:* An essential principle of a management policy for recorded information is that information is managed as a corporate resource and not as part of the separate domains of individuals, divisions or schools.

3. *Adopt a life-cycle management approach:* Sound principles for information management are based on the life-cycle approach. Management activities within the life-cycle encompass the planning of information systems; appropriate controls over the collection, creation or compilation of recorded information; establishment of practices and procedures governing the organization, distribution, retrieval, use, accessibility and transmission of the recorded information and for its storage, maintenance and protection; provision for routine access and dissemination of such

information, as appropriate, and regulating the disposition of all recorded information.

4. *Assign accountability:* The *FOIPP Act* permits the delegation of responsibilities of the head under the legislation to other persons. Given the close relationship between FOIPP and the effective management of recorded information, there should be a similar delegation of accountability and responsibility for the management of the recorded information.

Beyond principles, there are certain basic requirements or directives relating to both the management of recorded information and FOIPP that should be set out in policy. School jurisdictions should include several directives in their policy for the management of information.

1. *A directive supporting life-cycle management:* The policy should set out directives requiring the school jurisdiction to plan, direct, organize and control recorded information throughout its life-cycle, regardless of the form or medium in which the information is held.

2. *A directive for the establishment and maintenance of record-keeping systems:* A record-keeping system is an information system that captures, maintains and provides access to records over time. The policy should require the school jurisdiction to establish appropriate record-keeping systems based on their statutory and business requirements.

   Such systems should be controlled by a current, comprehensive and structured identification or classification system which provides an effective means for organizing, locating and retrieving all recorded information in the custody or under the control of the organization.

3. *A directive setting out the special rules for the organization and filing of electronic records:* Electronic records are subject to the *FOIPP Act* and should be managed as part of any program for the management of recorded information. Where electronic records are not copied and filed in a non-electronic record-keeping system, an electronic record-keeping system should be designed to ensure that:

   - records are named;
   - contextual transaction data (date, subject, officials involved, etc.) is preserved;
   - records can be authenticated;
   - there is version control;
   - records are classified and indexed for retrieval;
   - there are access controls; and
   - there are controls over the alteration of records, including audit trails on use, and processes in place to permit the disposal of obsolete records under approved processes and schedules.

   The directive also should deal with the management, retention and disposal of e-mail.

4. *A directive requiring the establishment and maintenance of a corporate inventory:* The policy should mandate the establishment of a corporate inventory which lists and describes all the recorded information in the custody or under the control of the school jurisdiction and attaches holdings of particular information to responsibility centres for purposes of accountability for their management.

   The inventory is a critical tool for the overall management of information. It should support the accessing of information both internally and externally to the public body and the application of privacy protection measures. The inventory also should serve as the basis for establishing disposition schedules and for descriptions for the *Local Public Body Directory of Records*, which must be provided to the Minister of Labour, as the Responsible Minister for the *FOIPP Act*, for publication. This also is true for the listing of personal information banks, which the school jurisdiction is required to maintain and make available to the public under Section 82(6) of the *FOIPP Act*. The corporate inventories may be in paper or electronic form and should serve as a locator system for all holdings of recorded information.

5. *A directive governing the creation and generation of records:* The policy should establish effective controls over the creation, maintenance and use of recorded information in the conduct of the business of the organization, through the establishment of a documentation standard which must be understood and followed by officials, employees and teachers of the school jurisdiction.

6. *A directive establishing a standard for transitory records:* Transitory records are recorded information that is not required to meet legal obligations or to sustain administrative or operational functions. Records required for statutory, legal, fiscal, administrative or operational purposes must be retained in a record-keeping system.

   Certain types of recorded information will qualify as transitory records: temporary information of short-term value (for example, notes kept to prepare official minutes of a meeting); duplicate documents; draft documents and working materials used to create a master record or which do not document policy changes or changes in decisions; personal messages and announcements. Much e-mail and voice mail that does not document a decision or transaction on behalf of the school jurisdiction qualifies as transitory records. School jurisdictions should have an internal e-mail policy that aids officials and employees in deciding when such recorded information should be retained in a record-keeping system.

7. *A directive dealing with the organization, retrieval and storage of recorded information:* There is a need to establish a framework for the operation of record-keeping systems in order that recorded information is organized and stored in ways which permit location and retrieval of the information and its appropriate security and protection, both for business and FOIPP purposes.

   The school jurisdiction should have standards in place relating to:

   - the organization, control and protection of recorded information, including electronic records; and
   - the storage of recorded information.

8. *A directive on the planning of information systems:* The application of information technology within organizations often has an impact on record-keeping activities.

   An information management policy should establish a mandatory process for introducing the record-keeping requirements discussed in this document into the planning and design of functional specifications for applications of technology which will collect, create or generate information used by the school jurisdiction.

   There are two special cases that go beyond the ordinary information management standards and specifications that should be considered in the design of information systems.

   The first is the need to support routine disclosure of information outside the *FOIPP Act*. Recorded information should be managed to promote public access when this is appropriate, including public access components that form part of information systems.

   As discussed in Part 2 of this study, school jurisdictions should ensure that opportunities for routine access to information and for actively disseminating information, when appropriate, are considered in the design and functional specifications for new or modified information systems, particularly when these are electronically based.

   Second, as dealt with in Part 4 of this study, there is a special need to consider privacy protection measures in the design and functional specifications for information systems which are used to collect, generate and manipulate and disclose personal information.

9. *A directive governing the disposition of recorded information:* Control over the disposition of recorded information is an important aspect of FOIPP administration. When responding to a FOIPP request, employees need to know if records have been destroyed and if this has been done in a legal manner. Likewise, in regard to the protection of personal privacy, it is essential to dispose of personal information under conditions that do not affect the privacy rights of the individual.

   All recorded information passes through phases of the life-cycle from creation to active record to inactive record and then to final disposition. School jurisdictions should establish a scheduling process that governs the disposition of all recorded information in their custody or under their control, including electronic records.

   A records schedule is a legal authority from the appropriate governing authority of an organization that outlines how long recorded information must be kept as it progresses through the phases of the life-cycle and establishes the final disposition of the record; i.e., destruction or archival preservation.

   School jurisdictions should establish a schedule to define and regulate the disposition of transitory records, including e-mail.

In regard to all recorded information, but particularly personal information, strict attention must be paid to the actual disposal processes. These should be governed by established and well-understood procedures.

All too often, sensitive personal information slotted for destruction is left in insecure conditions and thus is exposed to unauthorized access and, possibly, use; for example, garbage bags left in an alley which rip open and let loose documents containing personal information.

Used office and computer equipment poses a special risk. Sometimes filing cabinets are moved to an auction centre with files containing personal information still inside or computer hard drives or diskettes are similarly put up for auction without the information being wiped.

Disposal of paper and other hard copy media can be done by pulping or shredding. This should be done in established industrial facilities, which can attest that complete and secure destruction has occurred.

Computer hard drives and diskettes need to be professionally wiped clean of data before they are disposed of or sold.

10. *A directive concerning the management of recorded information in contracting:* Provision should be made in policy for all contracts to require the contractor to create records that meet the school jurisdiction's requirements.

    Contracts also should provide that the contractor will either maintain recorded information according to standards acceptable to the school jurisdiction, for as long as required, or pass them to the public body when the contract expires.

    When activities requiring the collection and/or handling of personal information are contracted out, the contract should set out the privacy protection obligations assumed by the contractor.

    Where information processing or other electronic data activities are contracted out, the contract should stipulate the information management and security requirements to ensure that the contractor meets FOIPP requirements.

    Conditions governing FOIPP and records management as they relate to contracting are further explained in the Alberta Labour publication, *Contract Manager's Guide to Freedom of Information, Protection of Privacy and Records Management in the Government of Alberta.*

## TECHNICAL INFORMATION AND DOCUMENT MANAGEMENT

Strong technical document management is essential to FOIPP compliance in electronic information systems.

1. *Analysis of documents:* There is a need to analyze documents from a FOIPP perspective to assist the instructional technology staff when they are preparing

documentation in a structured technological search environment (database) or making decisions on levels of security regarding employee and public access.

The FOIPP co-ordinator, in conjunction with information management and technology staff, should analyze and identify the records subject to FOIPP that are to be placed on an information system. These documents should be identified in terms of the FOIPP exceptions:

- *No exceptions to access:* No exceptions apply or discretionary exceptions are waived and the records are available for routine disclosure or active dissemination. Such records should be managed at the basic level of good information practice to ensure their integrity and availability to the organization and the public.
- *Exceptions to access:* The records relate to business interests, law enforcement or confidential internal business and need to be managed at a higher level of information practice and security to protect the confidentiality, integrity and availability of the records.
- *Personal information:* The information is personal information and thus subject to the special management rules set out in Part 2 of the *FOIPP Act* with regard to confidentiality, integrity and availability.

Such identification and designation of information holdings is essential to the planning of any information system, especially structuring downloading of files to the appropriate servers (for example, high security or public access) and to enable decisions on read/write access or no access, which govern the "need-to-know" principle for officials and employees within the information system.

When electronic personal information banks (PIBs) are identified under the *FOIPP Act*, it is essential that information technology staff are informed and asked to review information management and security controls to determine if they meet the requirements of Part 2 of the *FOIPP Act*. If there are deficiencies, these should be addressed as part of the remedial plan for implementing privacy protection measures. (See "Review of Existing Personal Information Systems" in Part 5 of this study.)

Chart 9 in Part 6 of this study provides a Security Summary Table for information systems.

Information technology staff must be made aware of their information management responsibilities. Responsibility and accountability should be assigned for any document management or record-keeping systems. This may fall to information technology staff or to an information management specialist. In any case, information technology staff need training and exposure to the rudiments of indexing and classifying records and to document management courses to increase expertise in systems document management.

The FOIPP co-ordinator or the accountable official for information management should provide guidelines for the maintenance of electronic records so that authoritative versions of records are maintained which have the context and integrity to document an activity or transaction.

2. *Electronic forms and templates:* School jurisdictions should create a graphic standard for the electronic forms, memos, correspondence or other materials that are to be placed on information systems. In some instances, there will be a need to place a privacy notification on some forms used to collect personal information directly from individuals in accordance with Section 33(2) of the *FOIPP Act*. In all cases, basic contextual information (source, date, electronic addresses, etc.) should be automatically inserted, as well as, where appropriate, security tags; for example, unrestricted, protected, confidential, etc. An information management policy should put in place an accountability structure to ensure that privacy statements are included on electronically-based or generated forms, which are often generated on a decentralized basis.

   When new forms of software are under consideration, one of the specifications should be that it permits the easy addition of privacy statements in ways which are convenient and which effectively inform individuals filling out the electronic form of their privacy rights. When consideration is given to self-service computer-based systems, provision should be made for pop-up screens and special modules that deal with the privacy notification requirements.

   Provision should be made for obtaining the individual's signature authorizing collection and use of the information on electronic forms when there is a need to demonstrate that the individual has full knowledge of the uses to be made of the personal information being collected.

   Any system should be able to provide a hard copy of the form to the individual, which includes the notification of collection. The organization should be able to retain a copy of the authorization and notification.

   These practices establish an audit trail within electronic information collection for the authorization of collection, the source of the information and the notification of collection and use. If these practices are not used, then some type of similar paper-based system should be in place.

   The information management policy also should include:

   - standards of documentation that clearly indicate that records created in documenting the activities or transactions may not be altered or destroyed without written approval of senior management. Alteration or destruction of records can be a very serious matter, especially if it is done to evade a FOIPP request, and should be the basis for disciplinary action;
   - an electronic retention and disposal program for information systems. Cost-effective business practices dictate that the school jurisdiction have a systematic process for disposing of electronic data as they become inactive and are no longer needed for business purposes or the long-term operations of the organization; for example, to protect the organization's interest in litigation. From an information technology perspective, such organized disposal can support a more efficient program of hardware purchasing. This should include a definition of "transitory record" within the information technology domain that governs an approval process for deletion of such records from information systems.

This process, known as electronic records scheduling, has several advantages from a FOIPP perspective. It provides control over records disposition, including transitory records, so that the organization knows what was destroyed and when and that employees are not searching for records that no longer exist. It also provides an official approval process for the disposition of records based on business needs that can be referred to when an applicant requests records that have been disposed of by the organization. Finally, it moves records through the system, thus reducing the exposure of the public body for requests for older records, which may be very labour intensive to deal with.

**_Basic Questions_**

The following questions are relevant to FOIPP and information management issues.

❑ Does our organization have in place an information management policy that:
- applies to all records;
- is based on the management of information as a corporate resource;
- adopts a life-cycle management approach; and
- assigns accountability for record-keeping systems?

❑ Does our organization have effective management and operational mechanisms for:
- supporting life-cycle management of information;
- establishing and maintaining record-keeping systems;
- organizing and filing electronic records;
- establishing and maintaining a corporate inventory;
- governing the creation and generation of records;
- establishing a standard for transitory records;
- dealing with the organization, retrieval and storage of recorded information;
- planning information systems;
- governing the disposition of recorded information, including electronic information; and
- managing information provided to contractors or which is required to be maintained by contractors?

## SECURITY

In order for information systems to comply with the varying components of the *FOIPP Act*, technical security and awareness issues must be appropriately managed. This section is not a technical discussion of security issues and approaches. Rather, it deals with management approaches and tools which will assist both the administration of effective security measures and the ability to meet FOIPP requirements, particularly those relating to the protection of personal information.

***Strategy***

Develop a security policy or administrative framework to govern protection of information and other assets within your school jurisdiction and to communicate security expectations and requirements to officials, staff and teachers. Policy requirements should be based on a technical security accountability framework. A technical security audit methodology should be planned as well as a methodology for assessing threats and risks. An assessment should be done of the current methods applied to installed technologies and the database collections of information.

## SECURITY POLICY

An essential first step in governing the development of security measures is to develop a security policy or administrative framework that sets out the requirements and expectations of senior management in regard to security. This should incorporate FOIPP requirements, particularly the need to protect personal information throughout its life-cycle, from its creation to its disposal, and from the earliest stages of the systems development life-cycle to ensure that such information systems reflect legal and policy requirements relating to privacy.

As indicated in Part 5 of this study, the *FOIPP Act* (Section 36) establishes fair information practices based on a sub-set of the life-cycle of personal information which requires that personal information be protected in regard to its collection and compilation, completeness and accuracy, use, disclosure and retention of personal information.

There also is a need to consider how other types of sensitive information (for example, business, law enforcement and internal operations information) which may qualify for exception under the *FOIPP Act* will be protected as regards its *confidentiality*, *integrity* and *availability.*

*Confidentiality* is the quality or condition of being sensitive (may cause injury if the information is disclosed).

*Integrity* is the quality or condition of being accurate and complete (may cause injury if information is modified, incorrect or incomplete).

*Availability* is the quality or condition of information, services, systems and programs being made available in a timely manner.

Another unique aspect of security in regard to FOIPP is the need to establish public access modules, based either on on-line access or use of the Internet, which are accessible to the public, but segregated from other organizational systems in order to protect the integrity of these internal systems and protect sensitive information from unauthorized access.

Essentially, the role of security is to help:

- ensure the availability of valid information when authorized users need it;
- protect the confidentiality of sensitive information held by the organization;
- protect the privacy of individuals whose information is part of the organization's information systems and of users of those systems;
- protect information assets from unauthorized modification; and
- ensure the ability of the organization to continue operation in the event of a disaster.

*Attributes of a Comprehensive Security Policy.* Many organizations have restricted security policies to one particular area, such as information classification, personnel security or information technology security. This sectoral approach to security works well to a point, but begins to falter when faced with the more global challenge of protecting a class of information, such as personal information. A security policy or framework should have the following characteristics:

1. *Authority:* A security policy should contain a statement of the authority or authorities under which the security policy is being issued and the expectation from the senior officer of the school jurisdiction as to its effective implementation.

2. *What needs to be safeguarded:* All assets of an organization, including information, require good basic care. Some assets, however, are more sensitive or valuable and require additional safeguards.

   A policy should include a requirement to carefully identify sensitive information, valuable assets and information systems that may need additional safeguards.

   Certain information will be excepted from disclosure under the *FOIPP Act* because it would reveal particular sensitive information or pose possible injury to public or private interests. These categories of information are generally described in the exception criteria of the *FOIPP Act*; for example, business, personal and law enforcement information and internal operations of organizations. School jurisdictions should take greater care in protecting these categories of information than they would information that is generally available to the public. Among these categories is personal information. The *FOIPP Act* defines personal information in Section 1(1)(n) and goes on in Section 16(2) to provide some guidance as to what types of personal information could pose an unreasonable invasion of privacy if disclosed.

3. *Information technology security:* The security of computer and telecommunications equipment and systems requires special consideration. This is due in part to the need to protect sensitive information, such as certain categories of personal information. It also is due to the significant extent to which many operations and services of organizations are dependent on such information technology.

   In addition to protecting the confidentiality of the information on these systems, it is necessary to define the importance of accuracy, completeness and availability to the management of the school jurisdiction's information technology systems. Defining the importance of the availability of information and services is the first step in making plans to resume business within an acceptable time and setting resource limits in the event of loss of data, systems or programs.

   It is important as well to identify potentially vulnerable communications systems. The risk of someone overhearing sensitive personal information on the telephone or through a data line should not be neglected, given the ease of accomplishing such access. Facsimile machines warrant special attention because of the chance of misdirecting sensitive information through an error in transmission.

4. *What safeguards are required:* The policy should require a threat-and-risk approach to security. This should include identification of what potentially requires safeguards and an assessment of threats and risks to this information, and to assets and information systems. This analysis provides the basis for assigning safeguards at a level commensurate with the risk. The security measures can be monitored and adjusted over time.

   The policy should:

   - require program areas to maintain complete and up-to-date inventories of personal information and personal information systems;
   - provide for the review of potential threats (for example, how sensitive personal information could be lost or changed, what impact this would have on client confidence in the programs, who would be affected and how); and
   - require the application of administrative, physical and technical safeguards and a personnel security program.

   Examples of *administrative, physical and technical safeguards* include:

   - written staff responsibilities and security procedures;
   - arrangements to resume operations in case of loss of computer-based data or capabilities;
   - use of physical barriers, security zones, access and authorization mechanisms and locked containers to restrict access;
   - use of proper containers and procedures for the secure processing, storage, transmission and disposal of information and other assets;
   - use of software, hardware or operating system access controls; and
   - use of secure communications and cryptography where the sensitivity of the personal information and the magnitude of risk warrant it.

5. *Personnel security:* Personnel security involves a process of checking the references and background of an officer or employee to ensure their reliability before

granting them access to sensitive information, information systems and the facilities involved with these, and/or permitting them to handle valuable assets.

Personnel security also enables implementation of the "need-to-know principle." That is, access to particular information or systems can be limited to certain officers and employees who need the information or system to perform their duties.

A security policy should set out some type of personnel security process.

6. *Breaches and violations:* A security policy should establish what would be considered breaches and violations of security. Section 36 of the *FOIPP Act* requires that among these are unauthorized access to, or collection, use, disclosure and disposal of personal information. The collection, use or disclosure of personal information, in violation of Part 2 of the *FOIPP Act* is an offence under Section 80(1)(e).

   A security policy should include a reporting mechanism, which requires that all violations and breaches be reported to the senior officer of the school jurisdiction.

7. *Sanctions:* The security policy should stipulate that the head of a school jurisdiction has the discretion to apply administrative or disciplinary sanctions for security breaches or violations. Sanctions, depending on the circumstances and the record of the officer or employee, may include the removal of access to sensitive information or information systems, verbal or written reprimand, suspension without pay or dismissal.

   As well, Sections 86(1) and (2) provide that a person must not collect, use or disclose personal information in violation of Part 2 of the *FOIPP Act* or destroy a record to avoid a FOIPP request. If they do, they are guilty of an offence and liable of a fine up to $10,000.

8. *Review and redress:* A security policy should ensure a fair and equitable process for treating individuals who have consented to personnel security checks or are subject to disciplinary action related to security. A clear process for appeal and review should be put in place.

9. *Security in contracting:* Protective arrangements under Part 2 of the *Act* apply to personal information in the custody or under the control of school jurisdictions which is collected, compiled, used, disclosed or disposed of by a contractor.

   A security policy should stipulate that its provisions apply to members of the private sector working under contract to the school jurisdiction and that they are required to handle personal or other sensitive information or to have access to information systems or facilities where such information is handled or stored. The extent of physical, technical and personnel security requirements that a contractor will have to meet will have to be decided on a contract-by-contract basis.

## TECHNICAL SECURITY—KNOWLEDGE, AWARENESS AND COMMUNICATION

Following is an overview of technical security problems that are extremely relevant to achieving FOIPP compliance for the protection of privacy and permitting public access.

*Source of Security Threats*. People can destroy information, executable programs, operating systems and other computing or system resources. Destruction can include both logical damage (to the system involved) and/or physical damage to the equipment itself. More interestingly, data can be altered to present the appearance of legitimacy.

People can steal information, the service or the hardware and software. This also could include the unauthorized use of system resources and removal and deletion of information as well as physical transport off-site.

People can disclose information to which they have no right or need, use it for personal gain or other motivations and let others use resources not intended for outside use. They can cause service disruptions or interruptions by causing physical or logical damage to the system and denying access to legitimate users.

While everyone seems aware of these types of issues, they do not often tend to think of security problems resulting from acts of omission (failing to do a backup) or accidentally causing a malfunction (repairs to software or hardware during working hours) or not complying with office policies concerning security because they are not enforced, out of date or just not done.

Other internal threats include damage by disgruntled employees, terminated employees who are still on site and ex-employees. Systems administrators, including LAN and database administrators, have special powers as they have global access. Damages can be serious and concentrated.

*Classifying Threat Sources*. To classify a threat source, it must first be decided if the threat is external or internal. External threats can be hackers, vendors or former employees. Internal threats can include disgruntled employees, unintentional losses or security breaches. Of the two, the internal threat often poses the greater danger.

*Types of Threats*. Threats to security can take the following forms:

1. *Interception of transmitted data:* Information in electronic form is often transmitted over telephone lines or by other electronic or physical means, such as diskette. These transmissions can take place between a storage device and a computer, between a data collection or data output point and a computer, or between one computer and another. This information, if not protected, may be intercepted or exploited, or just plain misdirected. It could end up in unauthorized hands and pose, at a minimum, embarrassment to a public body and, at worst, if at all sensitive, cause personal damage or injury to an individual.

2. *Unauthorized access to information:* Access to computers, particularly the mainframes or servers on which much personal information is stored, often is available through remote terminals. With increases in distributed databases, interoperability and networking, the possibility of an individual passing through

several electronic gateways to obtain unauthorized access has increased. The result of such penetration can be data theft, use of data for other purposes, alteration of data or data contamination so that the system lacks reliability, and the importation of bugs into a system so that it crashes or malfunctions.

3. *Portability of data:* Large quantities of electronic information can be moved physically from place to place in small packages, such as microcomputer diskettes or information on the hard drive of a laptop computer. When a computer is stolen, an entire system, complete with all its databases and access software, may be stolen as well. A whole system may be compromised.

4. *Ease of copying:* Information in electronic form is easily copied. Without adequate access controls in place, multiple versions of data may exist, making it difficult to ensure accuracy and to control unauthorized use, disclosure or disposal of personal information.

5. *Poor database design:* Often there is a tendency to assume that all users of a system need to have access to all information on the system. There may be very legitimate reasons for many users to have access only to discrete parts of personal information or only to do specific tasks or data transfer. Certainly, this was the case in a paper-based bureaucracy, and it remains true in an electronic one. There is, however, a fascination with getting as much data and information as possible on to each terminal. This is not always wise or prudent from a privacy perspective. Only as much information as is necessary to do a specific transaction or function should be available to the user. It is possible to design systems which discriminate between users on a protocol basis and suppress certain parts of files or certain fields. The design specifications, however, must carefully stipulate information flow and control of transactions.

6. *Ease of storage:* The length of time that personal information is kept on file is a concern in the privacy domain. Information in electronic form takes only a fraction of the space of paper documents, making it inexpensive to retain for long periods and increasing the possibility of out-of-date records being used to carry out an administrative action to the detriment of the individual.

7. *Hidden data matching:* In a traditional paper-based system, the ability to make logical connections between personal information in unrelated government files is limited by physical access to the files and the sheer number of documents involved. In an electronic system, access to several file systems can be gained from one location, and the speed at which computers can sort, select and compare data makes matching and linking of files a relatively quick and easy process. Add to this the fact that such matching and linking can be done by desktop and portable computers and the possibility of unauthorized use and disclosure of personal information for purposes detrimental to the individual increases exponentially. Chart 7 summarizes possible threats to computer resources (information, applications and equipment).

## CHART 7
## THREATS

| | |
|---|---|
| **Information**<br>Insiders (employees and contractors) | ♦ carelessness<br>♦ dishonesty<br>♦ inadequate training<br>♦ inadequate procedures<br>♦ human error<br>♦ mischief<br>♦ disgruntled employee |
| Outsiders | ♦ revenge<br>♦ former employees<br>♦ service staff<br>♦ hackers<br>♦ unauthorized access<br>♦ vandalism |
| **Computer Systems/Communications** | ♦ electronic entry/access<br>♦ eavesdropping/line tapping/scanning<br>♦ breakdown of carrier<br>♦ poor internal wiring<br>♦ system failure |
| **Software** | ♦ poor system development procedures<br>♦ poor testing of new and changed software<br>♦ poor maintenance procedures<br>♦ inadequate implementation |
| **Equipment and Premises** | ♦ poor lock-up procedures<br>♦ breakdown of equipment<br>♦ emanations<br>♦ poor premises services<br>♦ overheating |
| **Environment** | ♦ power failure<br>♦ high heat<br>♦ fire<br>♦ water/liquids<br>♦ natural disaster |

## CHART 8
## THE BASICS OF THWARTING UNWANTED EXTERNAL INTRUSION

In the networked environment, it is important to prevent and detect unwanted external intrusion into internal information systems. This is a particular problem where public access may be welcomed to part of the system.

| Action | What To Do |
|---|---|
| *Warn* | Using a log-in screen banner, system users and inbound callers using modems should be warned that the system is private. |
| *Check Passwords* | Review passwords for the obvious or weak ones. Change frequently. |
| *Build Systems Security* | Build security measures regarding systems and file access into hardware and software applications and into systems operations. |
| *Promote* | Post news stories about hackers and security breaches. This keeps security up front and in the user's mind and reinforces the fact that it can happen. |
| *Test* | Test published and known breaches in your own system. Are there procedures in place to prevent them? |
| *Monitor* | Track your long distance use. A sudden increase may mean a hacker is lurking in the system. |
| ***Keep your eyes, ears and mind open.*** | |

### DEALING WITH INTERNAL DESTRUCTION

Internal destruction is probably a bigger issue than external threats, primarily because employees already have access to premises, equipment and information. There is a need for senior management to carefully communicate expectations for appropriate care and security in the workplace while also communicating that willful destruction of all assets, including information, will be dealt with as a disciplinary matter.

The main cause of internal destruction is disgruntled or dismissed employees seeking revenge. As they know their way around the system, it is very easy for them to place "logic bombs" and other software bugs to corrupt the system's files long after they have left the job.

- At point of employment — The employee should sign a security agreement that defines the areas of the information system that the employee is permitted access to and those that are not accessible.
- Access denial — instructional technology management should be informed of an employee's release so that the person's access may be removed from all information systems. Timing here is crucial. If you do it too soon the employee will know; too late and the employee may be able to do damage.

*Role of the LAN Administrator.* In the modern networked workplace, LAN administrators manage one or more LANs, including hundreds of users on several servers, password assignments and files, backups, security and application access. They are in very powerful positions. To avoid vulnerabilities in this area, whenever possible:

- Divide responsibilities among other systems administrators.
- Have several individuals work together so that there is a wider exposure of operations.
- Ensure that back-up data are available off-site and controlled by other sources.

*Accidents, Mistakes and Unintentional Problems.* During the execution of the employee's performance of normal everyday duties, situations can arise that are created by accidents or mistakes or a lack of knowledge, experience or expertise in a particular area of information systems management.

Unintentional leaks can be as simple as:

- seeing a screen with a personal information bank on it.

  *Suggested solution:* Use screen blankers or screen savers that appear after a few seconds if the terminal is inactive. If the terminal is inactive for an extended period, and perhaps in a very public spot, install an automatic logout of the application.

- a person trying to find something on the system who accidentally finds a path through all the systems areas not normally accessible.

  *Suggested solution:* Staff should voluntarily bring such occurrences to the attention of the systems administrator. Staff should be informed about such a possibility and the procedures to follow—basically writing down what they did so that the systems administrator can try it.

- intense focus on one area of security to the detriment of others.

  For example, problems relating to the physical location of equipment may be overlooked. A person could find out how firewalls and security are set up and then come in from another direction that is not secured.

*Vendor Installation.* During the installation of an information system, the vendors may leave a back door or a trap door for maintenance. In a contract for services, there should be a clause specifying that these "doors" are closed. If there needs to be a maintenance port, all parties concerned should agree upon it and the appropriate security controls should be put into place.

*Dealing With Viruses.* A virus is a computer program that copies itself by attaching to other programs, thereby "infecting" them and performing unwanted actions. They are posing an increasing threat to the electronic work environment as officials and employees reach out to download documents, share work and send e-mail over widely shared networks. Viruses should be handled in two ways: by having sound policies and procedures which officials and staff must follow for downloading data and for handling of diskettes and other electronic media that could infect an information system by transfer; and by using antivirus software.

## BASIC PROTECTION MEASURES FOR SENSITIVE INFORMATION

1. *Encryption:* Encryption, which transforms clear text into an unintelligible form, is used to protect personal and other sensitive information that might fall into unauthorized hands. It is the fundamental safeguard at the base of a wide variety of security products, systems and mechanisms, such as secure facsimile, secure telephones, some computer products and software encryption devices for hard disks, diskettes, personal computers and laptops.

2. *Authentication and personal identification numbers (PINs):* An essential security control is authentication of those who can access and use an information system. Traditional system authentication has been a password at varying levels of complexity. Passwords are, however, open to compromise and other devices are now being used for more sensitive information. Smart cards are the latest in a generation of transaction cards. A smart card looks like a conventional bank or credit card, but it contains an integrated circuit chip. The chip embedded in the card can process and store data. Each card can support multiple applications, and each of these can be secured from the others. For increased security and data integrity, the card is capable of encrypting data to be stored on it or data that is to be transmitted to a host computer. A PIN is a number intended to be known only by the cardholder. It is stored on the smart card. When users desire access to the computer holding their personal information, they insert their card into a terminal equipped with a smart card reader (similar to those used in automated banking machines to read magnetic strip cards). The terminal asks each user to enter their PIN and, if the number is correct, provides access.

## TECHNICAL ACCOUNTABILITY FRAMEWORK

There is a need for accountability for applying security measures to information systems. As we have seen, this goes much broader than FOIPP considerations, but they now must be an integral part of security measures, particularly in regard to document control procedures, the authorization process for access to any system (employee, contractor, public) and for the protection of aspects of privacy.

The Security Summary Table (Chart 9) provides general guidance for assessing security measures for electronic information systems.

## CHART 9
## SECURITY SUMMARY TABLE

| Legend<br>Basic: normal print<br>Medium: underline<br>High: shading | Increasing Protection<br>Basic - Medium - High | Increasing Uptime<br>Basic - Medium - High | Increasing Accuracy<br>Basic - Medium - High |
|---|---|---|---|
| **Procedural**<br>• **Administration**<br>• **Organization** | Assignment of responsibilities<br>Separation of duties<br>Classification procedures<br>System Development Life-Cycle<br>Standards policies<br>Business resumption plan<br>Statement of sensitivity<br>Security clauses in contracts | Log review<br>Backups and recovery<br>Written procedures<br>System Development Life-Cycle<br>Contracts of:<br>• Hardware<br>• Software<br>• Communications<br>Specify:<br>• Minimum downtime<br>• Critical minimum<br>Contingency planning<br>Business resumption plan | Change control<br>Media marking<br>Log procedures and review<br>Verification<br>Security audit<br>Testing |
| **Personnel** | Training awareness<br>Correct screening clearances<br>Termination procedures<br>Security clauses in contracts<br>Separation of duties<br>Need to know<br>MUTUAL ACCEPTABILITY<br>ACCESS VERIFICATION | Training<br>Designated employees<br>Backup personnel specified<br>Emergency Response Team<br>RECOVERY TEAM | Training<br>Job description<br>Job responsibilities<br>Termination procedures<br>ACCESS AUTHENTICATION |
| **Physical and Environmental** | Access controls<br>• Physical<br>• Logical<br>Doors correctly secured<br>Walls floor to slab<br>Waste disposal<br>INTRUSION DETECTION SYSTEMS<br>VERIFICATION OF AUTHORIZATION | Environmental controls<br>Fire protection<br>Off-site storage<br>ALTERNATE SITE | Environmental controls<br>Physical access controls<br>Transportation of media |

| | | | |
|---|---|---|---|
| **System**<br>• **Operations**<br>• **Hardware**<br>• **Software** | System access control<br>File access control<br>Separation of<br>• Development<br>• Testing<br>• Production<br>Trusted computing at an acceptable basic level<br>Separation of physical media<br>Transaction logging<br>Audit<br>Restriction of privileges and capabilities<br>Trusted computing at a medium level<br>ENCRYPTION<br>TRUSTED COMPUTING AT HIGH LEVEL | Maintenance<br>Change control<br>Inventory hardware/software<br>Off-site backup of both system software and data<br>Minimum configuration<br>Uninterruptible power source<br>Hardware redundancy<br>ALTERNATE FACILITIES (CONTINGENCY PLANNING) | Change control<br>Restriction of privileges and capabilities<br>Configuration control<br>Maintenance<br>Range checks<br>Value checks<br>Error detection<br>Error correction<br>CHECKSUMS<br>LOGGING - ERRORS<br>AUDIT JOURNALS<br>AUTHENTICATION |
| **Communications** | Configuration<br>Surveillance<br>Log review<br>Change control<br>Access control<br>Authentication<br>Approved encryption<br>HIGH GRADE ENCRYPTION | Configuration<br>Change control<br>Log review<br>Specify<br>• Minimum downtime<br>• Official minimum<br>Alternate routing<br>DUPLICATE SERVICES | Configuration<br>Change control<br>Surveillance<br>Error detection<br>Retransmission<br>Log review<br>AUTHENTICATION |

## TECHNICAL AUDIT METHODOLOGY AND PROCEDURES FOR SECURITY THREAT-AND-RISK ASSESSMENT

The security of computer and telecommunications equipment and systems requires special consideration. This is due in part to the need to protect sensitive information, such as certain categories of personal information. It also is due to the significant extent to which many government operations and services depend on such information technology.

Determination of the levels of security protection required for a particular information system normally is done through a threat-and-risk assessment. This is core to the security assessment that should be done for new information systems holding or processing personal information (see Part 5 of this study).

Identifying the sensitivity of information is one essential pillar of security in a threat-and-risk assessment, which melds sensitivity or confidentiality with the requirements for information or data integrity, quality and availability, in the context of what may happen to compromise a system or program. Done well, the threat-and-risk assessment can anchor a risk management approach to security. The nature of threats provides the main design criteria for security systems and equipment (see Chart 9). Furthermore, the useful life spans of security systems and equipment often are dictated by the technological advances available to those that would defeat a system. A complete and current assessment of the threat to information and assets is therefore needed to determine the adequacy of existing or proposed safeguards, both physical and technical.

Inappropriate safeguards may leave the information vulnerable to identified threats or, conversely, it may be overprotected. Both situations are unacceptable. Security measures should always be predicated on the balancing of vulnerabilities against threat-and-risk. This is simply a formula for managing risk. In Chart 10, threat-and-risk assessment is broken down into five broad steps.

## CHART 10
## HOW TO ASSESS SECURITY NEEDS

| | |
|---|---|
| **Identify Assets** | Identify data, networks, network components, locations of information. Prioritize networks in descending order from most vital to least. |
| **Identify Threats** | Itemize threats to the assets that you have listed. Assets not threatened need minimal protection. There is rarely a one-to-one relationship between threats and assets. |
| **Identify Vulnerabilities** | A vulnerability is the path a threat takes to get to an asset. Protective measures block such paths. Creative thinking and brainstorming can find vulnerability paths. |
| **Consider Risks** | A risk is the probability of a threat getting to an asset. |
| **Take Protective Measures** | Protective measures block vulnerability paths and so reduce risk. Multiple measures may cumulatively improve or degrade overall security. There may be financial, legal or moral limits to protective measures that can be taken. It may be less costly to fix the problem afterward than to prevent it. Sometimes pre-emptive extended security measures are implemented because they are easy or inexpensive to do at the time. |

Chart 11 provides a summary of the steps involved in evaluating security for a network application.

## CHART 11
## EVALUATING NETWORK SECURITY

| | |
|---|---|
| **1. Gather Data** | Take an Audit (Inventory)<br>• Data<br>• Networks<br>• Equipment<br>• Protocols<br>• Traffic |
| **2. Analyze** | Perform a Risk Assessment<br>• Automated<br>• Manual<br>• Anti-Piracy<br>• Loss Scenarios |
| **3. List of Tasks** | Requirements/Statements |
| **4. Implement** | Hardware and Software Acquisition(s)<br>• New and Updated Policies<br>• Network Operating Security Options |
| **5. Integrate** | Network Security<br>• Business Continuance Plan<br>• Disaster Recovery Plan |

### ***Basic Questions***

In dealing with security of information, particularly personal information, the following questions are relevant.

□ Do we have a comprehensive security policy in place to govern activities related to the availability, confidentiality and integrity of our information systems?

□ Do we integrate security assessments designed to aid in the protection of personal privacy into the planning and design specifications of new or modified systems dealing with personal information?

□ Is responsibility and accountability for the management of security issues and implementation of protective measures effectively assigned within our organization?

□ Do we use a threat-and-risk assessment approach to determine the nature and extent of protective measures required for information systems?

□ Do we assess the security risks and take effective measures to protect our internal systems from penetration by external users through our own public access systems and interactive networks such as the Internet which are used by our employees and students?

## E-MAIL

Electronic mail, or e-mail, is a digital form of communication that allows messages and documents to be sent from one computer to another. It is fast becoming a major tool by which officials, employees and teachers communicate among themselves. It is used extensively by students and is now, in some instances, being expanded into a two-way communication with the public.

It is a crucial part of the link onto the Internet, with its world-wide messaging and document transfer system. E-mail allows rapid transmission of information without the frustrations of playing telephone tag and permits the sender to transmit more information than through telephone answering or voice messaging systems. It wipes out distances and time zones between offices, and speeds up decision making by "leap frogging" the traditional hierarchies in organizations.

Users tend to equate e-mail with the notes on a telephone response slip and do not give much consideration to the type of information that is being transmitted or its organization and security. Increasingly, however, besides simple messaging, such systems are used to distribute memoranda, circulate draft documents for comment, disseminate policy direction and guidance, transfer official records or carry out correspondence concerning the operation of organizations or the delivery of services, all of which merit more serious attention.

It is necessary to control the school jurisdiction's official records that are located on e-mail systems. These may well become the subject of a FOIPP request and may have to be produced for the applicant, unless they have been disposed of under an approved records schedule.

There also are privacy protection issues arising from the use of e-mail. One involves such a system's use to transmit sensitive personal information without proper security measures. The second involves the surreptitious monitoring of the personal e-mail of teachers, employees or students without a strong legal case for suspecting wrong-doing.

## E-MAIL AS A RECORD

E-mail sent or received over systems operated by or on behalf of a school jurisdiction and relating to the business of the jurisdiction are records subject to the provisions of the *FOIPP Act*. In addition, any personal information collected through or compiled on an e-mail system in the course of school jurisdiction business is subject to the privacy protection provisions set out in Part 2 of the *FOIPP Act.*

Officials, employees, teachers and students use e-mail systems in school jurisdictions for private purposes. However, by virtue of being created or received on school jurisdiction systems, such messages fall under the custody and control of the school body. School jurisdictions should endeavour to put in place practices and procedures which protect the privacy of individual e-mail users; for example, explicit rules on monitoring and copying a user's messages. Normally, monitoring and copying of messages should be done only for cause; for example, where there is evidence that an illegal activity may be taking place.

**Strategy**

Develop a policy on the use and management of e-mail for your organization, which takes into account the requirements of the *FOIPP Act*.

## E-MAIL AND PROTECTION OF PRIVACY

Most e-mail systems are designed with a minimum of security features in order to promote ease of use and communication. For this reason, it is generally not a wise decision to use e-mail utilities to collect, disseminate and use or disclose personal information, the unauthorized release of which could be harmful to personal privacy. In the instances where a messaging system must handle personal information, a privacy impact assessment, as suggested in Part 5, should be undertaken and measures put in place to ensure that privacy protection requirements of the *FOIPP Act* can be met.

## MANAGEMENT OF E-MAIL AS RECORDED INFORMATION

E-mail is a record for purposes of the *FOIPP Act*. For this reason, it must be managed in the same way as other recorded information. There are, however, several anomalies with e-mail that make this process more complicated and challenging.

E-mail systems do not distinguish between records of ongoing legal, fiscal, audit, administrative and operational purposes and more transitory records such as personal messages, announcements of social events, copies or extracts of existing records and message slips. The system itself and the complementary records management procedures should be designed to ensure that the identity, purpose, and location of records are predictable, consistent and reliable; that methods for access and retrieval are simple and well-defined; and that records management practices are incorporated into day-to-day business activities.

Procedures should be in place requiring users to segregate records of enduring business value from records that should be discarded on a regular basis in order to ensure that the system does not become clogged with extraneous records which do not reflect the transaction of public business. Most systems provide a discipline for this process by either automatically removing all e-mail that has remained on a system for more than a specific period of time (for example, three days or one week) to archive or back-up systems or to actually purge the system of e-mail at particular points in time. This latter process should be governed through an organization-wide transitory records schedule or policy.

E-mail records should be considered as documenting the organization's business when they are created or received as part of the transactions or operations of the school jurisdiction and contain evidence of its official policies, actions, decisions or activities or those of staff and teachers. Other e-mail records may contain valuable informational content on an event, organization or activity that involves the organization. Such records also should be considered as records documenting the organization's business.

The vast majority of information on e-mail systems comprises transitory records. *Transitory records* are defined as records in any media that:

- have only temporary usefulness;
- are not part of an administrative or operational records series;
- are not regularly filed in a records or information system; and
- are required for only a limited period of time for the completion of a routine action or the preparation of a record.

Transitory records are records that are not required to meet statutory obligations or to sustain administrative or operational functions. Records required for statutory, legal, fiscal, administrative or operational purposes should be retained in a regular records or information system.

## OPTIONS FOR MANAGING E-MAIL

There are three basic options for managing e-mail records. School jurisdictions should choose the method which meets their business needs, including those of users, and which can be most easily integrated with its overall record-keeping strategies and requirements. Once a method has been chosen, all users must be aware of the new policies, procedures and tools and be capable (through training and help systems) of applying them to all e-mail records.

1. *Management within e-mail utility:* Many e-mail users attempt to manage and store records within the mail utility. Most e-mail packages allow users to design personal filing systems using electronic folders and other similar methods. Users can move incoming messages from their in-box to appropriate folders, establish work queues, request notification from the system based on the status of an action or document and create automatic deletion routines. This approach provides a powerful tool to help users manage large volumes of e-mail messages consistently and automatically. It is particularly useful in managing transitory records.

   However, this approach fails to meet several requirements for the proper management of records. In most e-mail utilities, each end user controls his or her messages, which are inaccessible to others who may need to access them. Both compliance and consistency are difficult to achieve because end users have a great degree of discretion regarding how to design and use the filing functions. Space limitations or restrictions on the number of messages that each user is allowed to store further limit the effectiveness of this approach for retaining records.

   While e-mail handling features are valuable personal productivity tools, they are not adequate for filing, retention, access or protection of records documenting public business. For that reason, it is recommended that the e-mail system itself be used to manage only transitory records. One of the other options outlined below should be used to manage records documenting public business.

   Where a process is in place to segregate records documenting school jurisdiction business from transitory records, end users may delete records from the system at their discretion or employ auto-delete/archive functions in the system to eliminate transitory records from the e-mail system automatically; for example, on a weekly, monthly or other cycle appropriate to the public body and the system.

Transitory records that do not support business purposes should be destroyed in a timely manner. When such records accumulate in e-mail systems, they consume network and disk space and erode the efficiency of the system. As well, such records may fall within the scope of a FOIPP request or other procedures such as legal discovery.

2. *Print and file records in manual systems:* Another option for storing e-mail records which document public business is to print them on paper or some other medium and file them in existing filing systems. This option is easy to implement, especially where well-designed filing systems already exist. It also is an effective way to integrate the handling of paper and electronic records in applications where the records are created and received in both hard copy and electronic form.

   The records printed and filed in manual systems are managed and scheduled for disposition as part of the existing records series.

   This option has several disadvantages. The ability to search for, retrieve or retransmit documents electronically is lost if records are deleted from the e-mail system after printing. Complete compliance is hard to accomplish if end users are responsible for printing, routing or filing their own messages. As well, the approach can be costly because staff are needed to print, organize, file and retrieve records. If this option is chosen, it is essential to print all address, recipient, distribution, transmission, and receipt information needed for authentication with the content of the records.

3. *Electronic filing system or repository:* The third option is to design an electronic filing system or repository where e-mail records documenting school jurisdiction business can be stored, accessed and managed under the controls established by the public body and in accordance with government-wide records management policies, standards and procedures.

   This option has the advantage of providing a consistent method for organizing and retaining electronic records. If the filing system or repository is designed well, kept up-to-date and secure, it provides all authorized users with easy and consistent access to records. Measures can be put in place for naming documents, version control and authentication that make it easy for users to locate a record in the version needed and to ensure that records retrieved from the filing system have not been altered. The repository can be designed with controls to prevent unnecessary duplication of records and permit regular removal of records that no longer serve a business purpose. These records should be disposed of through an ongoing records schedule.

   The main disadvantage of this approach is that program staff and network administrators must plan for and design a filing structure that can adequately support operational needs and record-keeping requirements. Unless the business process is fully automated and all records are in electronic form, it will be necessary to co-ordinate filing systems for records in paper and other media with those in electronic format. If the filing system or repository is large and complex, specialized staff may be needed to classify, organize, maintain and dispose of records in the system.

Technological restraints and practical considerations may prevent school jurisdictions from retaining e-mail records in electronic filing systems at this time. However, public bodies are encouraged to adopt electronic filing practices whenever possible, especially when office systems are updated or redesigned. The benefits of electronic filing systems include better integration of records into work processes, ease in locating records, reduced handling and storage costs, and more automated and accurate handling of the routing, storing and disposition of records.

## STANDARDS FOR MANAGING E-MAIL RECORDS IN ELECTRONIC FORM

The school jurisdiction's management of non-transitory electronic documents created or received on e-mail systems should provide adequate documentation and meet records management and disposition requirements. Following are particular standards relating to identifying and preserving electronic mail messages that are non-transitory government records:

1. Transmission data providing the context of the record must be preserved. At a minimum, this will involve the names of the sender and addressee(s).
2. Organizations must preserve directories or distribution lists of users in e-mail systems for purposes of identification.
3. Instructions must be issued to users on when to specify that receipts or acknowledgments are required for record-keeping purposes and how to preserve these.
4. Where e-mail systems transmit messages outside the school jurisdiction, reasonable efforts should be taken to capture the transmission and receipt data needed by the jurisdiction for record-keeping purposes.
5. Calendars and task lists are records that should be maintained.
6. E-mail records should be grouped into related subject classifications according to the nature of the business purposes the records serve.
7. Easy and timely retrieval of records and subject filings of related records needs to be planned.
8. E-mail records must be retained in a usable format for the period of time stipulated in a records schedule approved by the organization.
9. E-mail records must be organized and available to all authorized personnel who have a business need for the information in a particular grouping of records.
10. School jurisdictions should not store the record-keeping copy of e-mail messages only in an e-mail system or on back-up systems unless those systems meet the above standards and qualify as record-keeping systems. If the e-mail or back-up system is not designed to be a record-keeping system, staff should be instructed on how to copy non-transitory records from the e-mail system to a record-keeping system.

## SPECIAL CONSIDERATIONS FOR E-MAIL SYSTEMS

Some special considerations should be borne in mind when establishing a framework for managing e-mail records.

1. *Does the e-mail utility have sufficient document management capabilities to support routing, indexing, filing and deleting of e-mail messages?* Many e-mail packages include features that make it possible to distribute messages to groups, organize messages into folders, move messages to files or document management systems, and print messages for filing in manual systems. Some software packages capture standard subject items, document types, version data, software requirements and other identifying information with the message or document, and provide for automatic routing, deletion or removal of messages to off-line storage based on predefined conditions. When considering an e-mail system or application or the upgrade of an existing utility, selecting e-mail software with these capabilities and setting up the system or application to exploit them can automate many aspects of the management of e-mail. Use of such features reduces the amount of human intervention needed to manage e-mail messages and documents, promotes the consistent handling of records and reduces errors in filing and routing.

2. *Can the e-mail system support identification and authentication of records transmitted through e-mail systems?* Systems can be set up so that they create message or document profiles automatically. The profiles identify the record creator, transmission and receipt date and time, recipient and status. If e-mail messages are to be used as evidence of the transaction of an organization's business and recording of decisions, this data must be captured with an e-mail message to ensure that the sender is who s/he claims to be, that the message actually was sent, and that it was received and viewed by the recipient. Some e-mail packages have the capability of capturing this authentication data automatically while others may require customizing to satisfy authentication requirements.

3. *Have naming conventions for business operations and document types been developed?* Naming conventions for business functions, applications, file folders, documents and document types support accurate filing and consistent retrieval of records. Naming conventions help users organize incoming and outgoing messages and decide where to route or file e-mail messages. Consistent use of naming conventions also enables automatic routing, sorting, filing and deleting of e-mail.

4. *Have standard forms and formats for document types been developed?* Often called document templates, standard forms and formats for documents such as letters, memos, requests and reports aid in identifying records and integrating them with the appropriate business function. Many e-mail software systems support templates or style sheets for different types of documents and have electronic forms capabilities. Use of these features provides a consistent structure and appearance for specific types of documents and facilitates automatic routing, classification and filing of electronic documents.

5. *Has the use of document profiles been considered?* Document profiles in message headers, document headers or cover forms enable users to create an abstract of the

content or other features of electronic documents. Document profiles identify the author, owner and subject of the records, and support automated search and retrieval.

When planning and implementing e-mail systems or applications, school jurisdictions should consider records management requirements in the selection of software and other technical equipment and in the establishment of policies, practices and procedures governing the operation of the system or application.

## E-MAIL AND FOIPP REQUESTS

E-mail may be subject to access requests under the *FOIPP Act*. To meet the statutory requirements of the legislation, searches for records responsive to a particular request must include all records filing and information systems, including all those where e-mail may be stored.

For this reason, it is important to delete transitory records from e-mail utilities and destroy back-up tapes in an efficient and organized manner, after records documenting public business have been selected and segregated for longer term retention. Deletion of e-mail requires both the sender and the recipient to delete the message.

The application of the *FOIPP Act* to deleted records captured on back-up tapes is less clear. A case can be made that this situation is similar to paper or other records that are awaiting destruction but have not yet been destroyed. In this latter instance, the records would have to be searched and any responsive documents retrieved. E-mail back-up tapes are, however, more sporadic and generally lack the organization to make such a search and retrieval either a certain or easy matter.

The deletion of records on e-mail systems varies widely. A school jurisdiction should make the procedures, requirements and effects of deletion clear to users in its corporate e-mail policy.

Generally, e-mail systems operate in one of two ways. Some systems allow a user to delete a record immediately so that it is not actively stored anywhere. In some systems, there is no back-up tape record of the e-mail. Other systems permit the deletion of e-mail, but it is deposited in the “old read file” or “old outbox" for a period of time (usually one to sixty days) and held possibly longer on back-up tapes. Where the e-mail exists in the “old read file” or “old outbox,” it can be recovered very easily. Such records should not be considered deleted government e-mail and should be considered as accessible under the *FOIPP Act.*

Whether or not deleted e-mail should be subject to search and retrieval procedures under the *FOIPP Act* should be considered on a case-by-case basis. But where a school jurisdiction receives a request dealing with deleted e-mail that has been properly disposed of under officially approved practices and procedures, officially the e-mail should not be considered a record for purposes of the *FOIPP Act.*

However, once a FOIPP request is received, all destruction and deletion of e-mail records, including back-up tapes that may contain responsive records, must cease until the records which are the subject of a request have been located and retrieved and the request completely processed. This is the same practice as is required for records in other formats.

## SECURITY OF E-MAIL

Security is a relatively difficult subject in the e-mail environment. As indicated in the discussion of protection of privacy, most systems are designed for open communication. Most e-mail systems will employ some standard security measures such as access controls, authentication of users, confidential mailboxes and activity reports. There is, however, little protection from the interception of messages, except in rare instances where the information being communicated is so sensitive that it is encrypted. Most e-mail systems do not have this feature and current encryption technologies, apart from cost, are still at the stage where they slow down the operation of the system and discourage the frequent use that is desired by organizations.

Beyond interception of messages, there are more prevalent threats from users that centre on the simple misdirection of documents, failure to stipulate a confidential mailbox or distributing a document generally when it was intended for particular individuals on a need-to-know basis. As well, erasing a message in an e-mail system does not necessarily mean that the record is destroyed. Thus attention needs to be paid to the path that deleted data may take to back-up systems in order to ensure the security of deleted records.

School jurisdictions should take all appropriate physical and technical security measures to protect information transmitted over e-mail. Where there is a basic open system with only standard protective devices, users should not use the system to transmit or receive sensitive personal information or information such as minutes of in-camera meetings and confidential business information that would not normally be released under the *FOIPP Act.*

If an e-mail system will be required to transmit more sensitive and confidential information as part of its functionality, a public body should conduct a threat-and-risk analysis to determine what additional equipment, software and procedures (for example, encryption devices and enhanced user authentication) will be required.

Most e-mail systems defend against unauthorized access through user identification and authentication. This may be a password or number or a bar code, magnetic swipe card or a smart card. As long as the password or card is not compromised, then basic protection for the user and information is achieved.

More sophisticated systems will incorporate better authentication procedures (or encryption of information so that it can be read only by the sender and recipient) or communications security to deter and detect hacking (gaining unauthorized access) of the system. In the case of e-mail, one security measure to prevent both outside and internal compromise of a system is to disperse e-mail administration over several local area networks to segment what can be found out at any one server.

To ensure the security and authenticity of records communicated through e-mail systems, networks and e-mail applications must have access and security controls that restrict who can read, write, change and delete files. Today's networking and e-mail systems offer many options for supporting controlled, secure and reliable communications. Among the basic security considerations that should be spelled out in policy are:

1. *Password protection:* Passwords or other access controls protect the system or application from unauthorized users. The policy should emphasize that the use of passwords in an e-mail system is the shared responsibility of the network administrator and users. Some basic requirements should be spelled out, such as the need to:

   - choose passwords that are difficult to guess from the context of the individual or operation,
   - refrain from the sharing or disclosing of passwords,
   - keep track of previous log-ins to detect unauthorized use,
   - limit the number of consecutive log-in attempts, and
   - change passwords on a regular basis.

   Consideration also may be given to having the network administrator restrict access privileges, in some instances, to specific individuals who are authorized to participate in a particular business process or project by limiting rights to create, send or alter messages in specific directories, sub-directories or files.

2. *Message protection and authentication controls* prevent users from changing an e-mail message once it has been received by at least one recipient. These controls require users to send a new message with new transmission and receipt data if they wish to change the content of a message. The use of these control measures should be explained to users as a vital support within the system or application for the authentication and version control over electronic documents.

3. S*ecurity labels:* Protocols for the use of security labels such as "urgent," "confidential," or "acknowledgment requested" should be explained to users. Such labels can be attached to e-mail messages by the sender to alert recipients of special privacy or security handling requirements. The policy should set out circumstances where these measures may be employed and the practices to be employed in particular circumstances.

4. *System audit trails* automatically record the circumstances surrounding log-in attempts, creation, transmission and receipt, filing and retrieval, updates and deletion of messages in an e-mail application or on a network. Such practices should be employed where business needs make them appropriate, and users should be informed about them. Even the best designed security measures are vulnerable to unauthorized access and use. Therefore, systems should be designed and operated in ways that provide audit trails for monitoring a system's performance, ensuring that records management and security procedures are being followed and auditing transmission of messages in the system.

Other security measures such as encryption, virus protection and back-up procedures provide additional protection against unauthorized access, alteration or loss of records. To the extent these measures are employed in an e-mail system or application, an e-mail policy should explain their nature and the conditions under which they are applied.

Security measures can be costly to design, enforce and monitor. Program managers should be required to identify "high-risk" e-mail systems or applications and to work with network administrators and information technology security personnel to identify the sensitivity of the information to be carried on an e-mail system or application and to assess the threats and risks to which it may be exposed. Actual security measures should be based on this assessment.

In many instances, security measures will prove expensive to install and may detract from the overall ease of use and functionality of the system or application. In instances where the decision is to leave e-mail security at a rudimentary level, users should be informed that the e-mail system is for work-related, non-confidential messaging which forms the bulk of requirements in a work day and not sensitive information to which there is an absolute need to control access and hold confidential; for example, the notes of a cabinet meeting or sensitive meeting of senior officials. This is particularly true where an e-mail system is an open one, involving participation by the public, or has an interface to a public network, such as the Internet. Where practical, a list of the types of information that should not be communicated over the e-mail system should be provided to users.

## RESPONSIBILITY FOR E-MAIL

Individual officials, staff and teachers, as end users, are ultimately responsible and accountable for the appropriate use of e-mail systems and for the application of the information management and access and privacy obligations inherent in the collection, creation, transmittal and receipt of such electronic records. There is a need for school jurisdictions to assure that they know, understand and have the tools to meet these responsibilities. Outside the defining of technical specifications for systems and general systems administration and information management support, there remain questions about who has ultimate responsibility and accountability for managing particular work stations on an e-mail system. This is especially true when determining how the equipment will be employed and what information will be purged.

At one level, it would seem appropriate that individual employees or teachers have this control. After all, they should be managing their own mailboxes and ensuring that the individual work station is functioning effectively as part of the network. This is particularly so when the large number of *personal* messages on most e-mail systems are taken into consideration. One report from the State of California found that more than sixty per cent of all e-mail messages were of a non-business nature.

E-mail systems thrive on the free flow of ideas. Most attempts to control the explosion of messaging result in employees abandoning the system. Conversely, when some tolerance is shown and combined with a little training and disciplinary pointers, the problem of personal use becomes less onerous because non-business communication between employees is kept short and to the point.

Since so much of the messaging has a personal twist, there is some value in having individual employees and teachers controlling what is saved for long-term retention. But if this is to be the case, these individuals must be aware of the type of information that should be retained. As the current policy makes clear, this is the information that is essential in initiating or conducting the school jurisdiction's business and which would normally find its way into corporate filing systems in order to provide continuity to the decision process involved. A simple rule of thumb is whether or not the electronic message is used to initiate a new activity within the organization, comment on or deal with management guidance about an activity underway or request an opinion on an activity of interest to the school jurisdiction. Or is the message from or about a parent or student who is transacting business with the school organization?

Deciding on what will or will not be kept is only one aspect of the end-users' responsibilities within the e-mail management framework. End-user e-mail boxes should be structured with a directory of file folders that parallel those portions of the corporate file systems relevant to the program or operation involved. There is a need for instructions to users to review the system each day and purge personal and transitory information, while moving important information into one of the file folders. There also should be a requirement to periodically copy or move these folders into more permanent files (paper, electronic or microform).

School jurisdictions are responsible for ensuring that employees understand internal e-mail management policies and appreciate that the proper management of e-mail is an integral part of their job. There should be serious consequences (for example, warnings and cautions to users, action to remove an abuser from the system or the possibility of disciplinary action) for the failure to use and manage e-mail records in accordance with statutory and policy requirements.

## INTERNAL POLICY FOR THE MANAGEMENT OF E-MAIL

An *e-mail policy* should be corporate in nature, thus governing operation of the e-mail system and providing guidance to users. The user portion may be broken out to serve as a staff policy or circular.

Since the operation of an e-mail utility is considerably broader than issues centred on FOIPP, the following outline covers some issues that go somewhat beyond these fields. The outline comprises suggestions and comments that will help school jurisdictions come to grips with policies and procedures to cover the operation of their e-mail systems. Not every organization will need to cover every component outlined here. Inevitably, overall approaches may seem complicated to public bodies that require only a basic, simple policy. School jurisdictions should adapt and revamp the components provided here to meet their business needs and level of complexity of operations.

1. *Nature of the e-mail system*: The policy should describe the actual environment where e-mail is being employed. There are at least four types of e-mail systems:

   - systems restricted to the management of an organization;
   - systems used by all officials, staff, teachers and students;
   - systems which permit wide access to other individuals and organizations (now the most common with the use of the Internet); and
   - systems which permit broad two-way communication with the public.

   The nature of the system is a major determinant in the protocols governing its use. If it must bear both a public and confidential interface, then measures also must be taken to ensure security of communications and protection of privacy.

2. *Purposes of use*: There is a need to state clearly what the purposes of the e-mail system are and that its records are under the custody of the school jurisdiction. The policy should define proper use of e-mail and set limits on personal use. It also should indicate the scope of communication intended (for example, with all managers, all employees, all teachers, all students, external clients, customers and suppliers, the general public) and whether the system is intended to foster open communication and consultation or easier, more convenient, but still relatively private communication among a particular group.

   This section also should indicate the norm for messaging. Most electronic messaging systems permit a more informal approach that cuts across the hierarchy of a public body. Indeed, this is one of the strengths and benefits of an e-mail system. But all systems should have a protocol of use which permits creative and free expression of views while meeting the norms of accepted behaviour such as avoiding excessive profanity, sexual harassment, long, acrimonious and public disputes or flooding the system with messages that are of interest only to one or a small group of individuals. Again, where appropriate, it should be stressed that intemperate or ill-considered statements may become public through access procedures.

   Where systems or parts of systems are public, there should be guidance as to what should be posted; for example, documents on which consultation is being sought, notes on meetings which may be of interest to a wider group, completed documents, etc. Equally, there should be a clear indication of what is not permitted to be posted or transmitted; for example, if the system is open, no sensitive personal information, no minutes of in-camera meetings, no business confidences, etc. There also should be a clear process for obtaining approval for such postings.

   To the extent that personal communications are permitted on an e-mail system, the policy should inform users that it is their responsibility, as both sender and recipient, to ensure that such messages are removed from the system. Otherwise there is no guarantee that they may not become accessible to others as the system is backed up and administered.

3. *Information management on system*: The policy should clearly state information management requirements for the system. For example, the policy should specify:

   - what are considered to be transitory records in regard to e-mail and procedures for dealing with these;
   - where and how non-transitory records will be filed and managed (i.e., within the individual e-mail system itself or as paper records printed from the system or as a part of a central electronic repository associated with the system or as part of a decentralized electronic filing system);
   - what security and back-up measures are in place for the e-mail system in order to protect records from alteration, loss or inappropriate destruction.

4. *Roles and responsibilities*: A section in the policy should address the responsibilities of managers, end users, support staff, network administrators, technical staff and records management staff in regard to the various aspects of managing e-mail.

All users should be charged with specific responsibilities. These would generally be comprised of the following:

- There is an expectation that e-mail will be limited to the purposes for which it was established.
- Users are expected to reply promptly to messages requiring action.
- Users remove personal and transitory records from personal mail boxes on a regular basis.
- All non-transitory records will be stored in the format and media required by the school jurisdiction and stored in ways that make them accessible to those authorized to know the contents and secure from unauthorized access and destruction.
- All e-mail records are protected from unauthorized release to third parties and protected from inadvertent loss or destruction through compliance with back-up requirements and procedures.
- Personal information on the e-mail system must be protected in accordance with Part 2 of the *FOIPP Act*, with appropriate explanation of what this implies for the collection, use, disclosure, retention and security of the personal information.
- Users are expected to meet all access requirements imposed by the *FOIPP Act*.
- All dispositions of e-mail records must take place in accordance with the approved records retention schedules of the school jurisdiction.

In order to prevent conflicting directives and confusion about responsibilities, the policy should identify the position or office responsible for each part of the policy, practices and operation of the e-mail system.

5. *Freedom of information*: The policy should clearly state that any records in an e-mail system are subject to the *FOIPP Act*. Staff and teachers should be made aware that they may be asked to search their e-mail box in order to locate information pertinent to a FOIPP request, though as stated above, information that already has been destroyed under a duly approved schedule need not be recovered.

   In addition, the policy should state that the same rules apply to e-mail as to other types of information subject to a request. No information pertinent to a request may be destroyed after a request has been received, even where approved schedules are in place. Since electronic messaging systems record decisions to delete information, it would be very easy for an investigator from the Office of the Information and Privacy Commissioner to track such actions. The best method is to have a good information management scheme in place that deals with the disposal of information on an ongoing basis.

   Further, the policy should include a clear statement and warning that, under Section 86(1)(e) of the *FOIPP Act*, all persons are prohibited from willfully destroying any records, including e-mail records, with the intent to evade a request for access to the records.

6. *Security*: The policy should be very clear about the security measures for the e-mail system, which protect both the user and the information on the system. For most widely used systems this is rudimentary and amounts, as one expert has claimed, to "the same security level as a postcard."

Among other things, the policy should indicate clearly to users:

- the level of security on the system;
- what types of information can and can not be transmitted on the system and the level of confidentiality that can be expected by users;
- expectations for password management and other security procedures on the system;
- any special conditions or procedures that apply when sharing information or drawing information from other databases outside the e-mail system;
- any special conditions relating to the deletion of e-mail (for example, automatic filing or no deletion until all recipients have deleted the message or copy); and
- system audit trails that are in place and their general function.

7. *Protection of privacy*: The policy should forbid the transmittal over an e-mail system of any personal information which could reasonably be expected to cause an unwarranted invasion of privacy to an individual and would normally be held confidential by the school jurisdiction, unless special measures are in place to protect such information. This is a fair rule for most circumstances, but in some instances messaging systems are specifically built to deal with the transmittal of personal information or have security features which could permit this from time to time. In these instances, policy should set out for users protective controls relating to the collection, use, disclosure and protection of personal information as set out in Part 2 of the *FOIPP Act*.

   Users should be required to undertake special orientation and training related to the protection of personal privacy and the application of the special measures designed to ensure that individual privacy is protected in the system or application and to formally indicate, in writing, that they understand the legal and policy requirements relating to the handling of personal information in this electronic format.

8. *Monitoring of system*: The policy should set out the conditions under which the system administrator and other authorized individuals will monitor individual e-mail boxes. These conditions should take into account the following factors:

   - users of the system have a reasonable expectation of privacy;
   - general monitoring of e-mail communications for unspecified purposes should not be allowed;
   - if monitoring takes place (for example, as part of employee performance evaluation or supervision of student activities), system users should be asked to help in designing the process, be fully informed as to the tools used and how they will operate, and how the collected information will be used;
   - there will be no secret monitoring or searches, except as permitted by law enforcement measures based on credible evidence of criminal activity or other serious wrongdoing; and,
   - all collection, use and disclosure of personal information involving an e-mail system will be done in accordance with the legal requirements of Part 2 of the *FOIPP Act*.

9. *Understanding*: An e-mail policy is effective only if it is disseminated to and understood by staff. The e-mail system or application itself can provide a powerful

tool for distributing policies to users. Periodic distribution of the e-mail policy by an organization on its system is a good way to reach all users. Systems administrators can design special banners or help screens with particular directives and practices relating to difficult issues such as privacy protection, freedom of information, or document retention.

Orientation and training should be offered on the general use of e-mail and special policies that relate to it. Users of the system should be required to indicate that they have read the policy and understand the terms and conditions that it imposes. There should be consequences for not following these various terms and conditions which range from warning to removal from the system to the possibility of disciplinary action.

10. *Authority*: A section of the policy should indicate under what authority the policy is being issued and identify an officer responsible for its administration and to whom questions and comments about the policy may be addressed.

### ***Basic Questions***

The following questions are relevant to e-mail management.

- □ Does our organization have in place effective policy and procedures to manage the e-mail system in line with the requirements of the *FOIPP Act*?
- □ Do staff, teachers and students understand the purpose and rules which govern e-mail systems in our jurisdiction and how and under what circumstances e-mail records may be deleted from the system?
- □ Do we have FOIPP procedures that provide for the routine search of e-mail systems when locating records responsive to a FOIPP request?
- □ Do staff and teachers understand the rules about communicating sensitive personal information by e-mail?

# APPENDIX A
# STRATEGIES FOR SCHOOL JURISDICTIONS

## ACCESSING GENERAL INFORMATION

- Continue and strengthen current methods of communicating with students, parents, employees and the public-at-large, and seek to expand this informal, non-FOIPP approach to providing information. Develop an information access policy that enables your organization to be proactive in providing access to information and to avoid reacting to demands for information through FOIPP requests.

- To the extent possible and where it is practical, employ information technology to support regular disclosure of information outside the FOIPP process in order to better meet educational objectives and avoid FOIPP requests, while implementing the spirit of the *FOIPP Act* for more open, accountable and transparent administration of school jurisdictions.

- Use electronic media and formats, including public networks, as appropriate and within budgetary constraints, in order to make information more easily accessible and useful to students, parents and the public. Such efforts, however, should not preclude those without access to computer technologies from accessing similar information by other means; for example, publications, library sources, etc.

## ACCESSING PERSONAL INFORMATION

- To the extent possible, provide means outside the *FOIPP Act* for individuals to access and, if necessary, seek correction of personal information about themselves. The same rules under Section 83 of the *FOIPP Act* apply. Normally, the non-FOIPP process should provide the same personal information as if the individual had made a FOIPP request. If individuals may receive more information about themselves through the FOIPP process, they must be advised that this is the case.

- When establishing information networks with public modules, consider the feasibility of incorporating authentication, encryption and other electronic commerce and security features that will enable you to undertake transactions involving individuals obtaining personal information about themselves from the system on a routine basis.

## PROTECTING PERSONAL PRIVACY

- Develop corporate privacy protection policies and procedures that enable you to:
  - establish a methodology for addressing privacy protection and related security issues in planning and establishing functional specifications for new or modified personal information systems;
  - review personal information systems and bring them into compliance with Part 2 of the *FOIPP Act*;
  - review forms used in the collection of personal information to ensure that they meet the collection and notification requirements of the *FOIPP Act*;

- establish a security policy which includes protection of privacy as one of its aspects; and
- identify and manage the data matching of personal information.

➢ Establish practices and procedures which provide for the consideration of the requirements of Part 2 of the *FOIPP Act* in the planning, design, development of specifications and implementation of information technology to new or modified information systems used to collect, compile, process, store, use, disclose or manipulate personal information.

➢ Require that a privacy impact assessment (PIA) forms part of the authorization for all information systems used to collect, compile, process, store, use, disclose or manipulate personal information. This document should be the basis for attesting to the superintendent that measures have been integrated into the information system to meet the requirements of Part 2 of the *FOIPP Act*. (A model form is provided in Part 5 of this study.)

➢ Establish policies and organizational structures that will facilitate the integration of privacy protection requirements and practices into the ongoing management of personal information systems and plan how to bring existing program activities and personal information systems into compliance with Part 2 of the *FOIPP Act*.

➢ Require that all data matching activities involving personal information be reviewed by the jurisdiction's FOIPP co-ordinator and, where appropriate, that advice be sought from the Office of the Information and Privacy Commissioner.

## FOIPP AND INFORMATION MANAGEMENT

➢ Ensure that the management of all recorded information in your organization, including electronic information, is governed by a corporate information management policy. This should be developed with the administration of FOIPP in mind and include appropriate references to FOIPP requirements in both the policy statements and the procedures, practices and standards used to implement the policy.

➢ Develop a security policy or administrative framework to govern protection of information and other assets within your school jurisdiction and to communicate security expectations and requirements to officials, staff and teachers. Policy requirements should be based on a technical security accountability framework. A technical security audit methodology should be planned as well as a methodology for assessing threats and risks. An assessment should be done of the current methods applied to installed technologies and the database collections of information.

➢ Develop a policy on the use and management of e-mail for your organization, which takes into account the requirements of the *FOIPP Act*.

# APPENDIX B
# BASIC QUESTIONS FOR SCHOOL JURISDICTIONS

## ACCESSING GENERAL INFORMATION

The following questions should be posed to the organization when dealing with issues over access to information.

- □ Does our organization currently have in its custody or under its control information that:
  - is in demand; and
  - the release of which in a proactive and informal manner would better meet the concerns of students, parents and the public for more open and accountable governance of our school, board or district?
- □ Could we release such information either on a routine basis or through active dissemination without compromising those mandatory interests, particularly personal privacy, which we are required to protect under the *FOIPP Act*?
- □ Do the current technology applications which we are undertaking or planning to undertake in the near future, including use of the Internet, adequately take into account the need for the routine disclosure or active dissemination of this type of substantive organizational records?
- □ Have we or are we going to automate the creation and management of our organization's manuals, handbooks or other guidelines that the *FOIPP Act* requires must be made available to the public? Have we recognized this requirement as part of the management application?
- □ Do we have an information access policy and an ongoing process in place to identify such sources of information and to ensure that they are made available in ways that meet our overall business objectives?
- □ Do we release such information in forms (electronic and paper) which meet the needs of students, parents and the public?
- □ To the extent that we permit public access to electronic information (for example, an Internet site), do we have adequate technical safeguards in place to ensure that no access is permitted to our electronic information systems beyond these public data sources?

## ACCESSING PERSONAL INFORMATION

To the extent that information technology is used to maintain student, employee and other such personal information, the following questions related to systems design and implementation are relevant.

- □ Have we identified all categories of personal information where we are required or empowered to release such information to the individual it is about or to another authorized person?

- ❑ Can we use routine disclosure methods combined with information technology applications to improve and simplify such access?
- ❑ Can we ensure through technical means that only the entitled individual or an authorized representative has access to the specific personal information about the individual?
- ❑ Are adequate safeguards in place to protect the personal information within the electronic system and during its communication?
- ❑ Are there non-FOIPP means by which someone can request correction or amendment of a record within the system?

## PROTECTING PERSONAL PRIVACY

In considering the implementation of the privacy protection requirements in Part 2 of the *FOIPP Act* for electronic information systems which store, manage, manipulate or communicate personal information, the following questions are pertinent.

- ❑ Is there a process in place to ensure that a PIA is conducted during the development of new and modified information systems?
- ❑ When a PIA is conducted, are we satisfied with the measures recommended to ensure the system meets the legal requirements of Part 2 of the *FOIPP Act*?
- ❑ Is this technology project of such a significant and/or innovative nature that it merits consultation with the Information and Privacy Commissioner?
- ❑ Is a process and reasonable schedule in place to undertake the review of existing information systems dealing with personal information and any related forms to ensure that each system is brought into compliance with the requirements of Part 2 of the *FOIPP Act*?
- ❑ Are all program areas and schools identifying all data matching referred to the FOIPP co-ordinator for review and approval?

## FOIPP AND INFORMATION MANAGEMENT

The following questions are relevant to FOIPP and information management issues.

- ❑ Does our organization have in place an information management policy that:
  - applies to all records;
  - is based on the management of information as a corporate resource;
  - adopts a life-cycle management approach; and
  - assigns accountability for record-keeping systems?
- ❑ Does our organization have effective management and operational mechanisms for:
  - supporting life-cycle management of information;
  - establishing and maintaining record-keeping systems;
  - organizing and filing electronic records;
  - establishing and maintaining a corporate inventory;
  - governing the creation and generation of records;

- establishing a standard for transitory records;
- dealing with the organization, retrieval and storage of recorded information;
- planning information systems;
- governing the disposition of recorded information, including electronic information; and
- managing information provided to contractors or which is required to be maintained by contractors?

In dealing with security of information, particularly personal information, the following questions are relevant.

❑ Do we have a comprehensive security policy in place to govern activities related to the availability, confidentiality and integrity of our information systems?

❑ Do we integrate security assessments designed to aid in the protection of personal privacy into the planning and design specifications of new or modified systems dealing with personal information?

❑ Is responsibility and accountability for the management of security issues and implementation of protective measures effectively assigned within our organization?

❑ Do we use a threat-and-risk assessment approach to determine the nature and extent of protective measures required for information systems?

❑ Do we assess the security risks and take effective measures to protect our internal systems from penetration by external users through our own public access systems and interactive networks such as the Internet which are used by our employees and students?

The following questions are relevant to e-mail management.

❑ Does our organization have in place effective policy and procedures to manage the e-mail system in line with the requirements of the *FOIPP Act*?

❑ Do staff, teachers and students understand the purpose and rules which govern e-mail systems in our jurisdiction and how and under what circumstances e-mail records may be deleted from the system?

❑ Do we have FOIPP procedures that provide for the routine search of e-mail systems when locating records responsive to a FOIPP request?

❑ Do staff and teachers understand the rules about communicating sensitive personal information by e-mail?

# APPENDIX C
# RELATED ALBERTA EDUCATION RESOURCES

*Computer Network Security: Best Practices for Alberta School Jurisdictions* (1999).

*Developing A Three-Year Technology Integration Plan: A Resource for School Jurisdictions* (1998).

*FOIPP and Technology Highlights: Best Practices for Alberta School Jurisdictions* (1999).

*Implementing and Managing Web Site Development in Education: Best Practices for Alberta School Jurisdictions* (1999).

*Managing Technology Funding: Best Practices for Alberta School Jurisdictions* (1999).

*Network Design: Best Practices for Alberta School Jurisdictions* (1999).

*On-Line Learning: Best Practices for Alberta School Jurisdictions* (1999).

*Preparing to Implement Learner Outcomes in Technology: Best Practices for Alberta School Jurisdictions* (1999).

*Professional Development for Teaching Technology Across the Curriculum: Best Practices for Alberta School Jurisdictions* (1999).

*Technical Support Planning: Best Practices for Alberta School Jurisdictions* (1999).

*Technology Implementation Review, Grande Yellowhead Regional Division No. 24 and Wolf Creek Regional Division No. 32: Best Practices and Key Learnings with Respect to Technology, Its Implementation and Management in Education* (1997).