DOCUMENT RESUME

ED 429 577 IR 019 538

TITLE	FOIPP and Technology Highlights: Best Practices for Alberta School Jurisdictions.
INSTITUTION	Alberta Dept. of Education, Edmonton.
ISBN	ISBN-0-7785-0342-9
PUB DATE	1999-02-00
NOTE	21p.; A publication of the School Technology Task Force. For related document, see IR 019 537.
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/PC01 Plus Postage.
DESCRIPTORS	*Access to Information; 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

The information in this document is based on a study that Alberta Education commissioned on establishing technology systems that are responsive to the requirements of Alberta's Freedom of Information and Protection of Privacy Act (FOIPP). This document provides an overview of key issues and suggested strategies in the following areas: (1) accessing general information; (2) accessing personal information and protecting personal privacy; and (3) FOIPP and information management, including managing records, security, and e-mail. Appendices include: a summary of suggested strategies for school boards with regard to FOIPP and technology; related definitions; privacy impact assessment guidelines; security summary table; guidelines for evaluating network security; and a list of related Alberta Education resources. (AEF)

FOIPP AND TECHNOLOGY HIGHLIGHTS

Best Practices For Alberta School Jurisdictions

February, 1999

Alberta
EDUCATION

ALBERTA EDUCATION CATALOGUING IN PUBLICATION DATA

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

Available on the Internet: http://ednet.edc.gov.ab.ca/technology/
ISBN 0-7785-0342-9

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

The information in this *Highlights* document is based on a study that Alberta Education commissioned on establishing technology systems that are responsive to the requirements of the new *Freedom of Information and Protection of Privacy Act* (*FOIPP*). The study, *FOIPP and Technology: Best Practices For Alberta School Jurisdictions* (1999), contains extensive and detailed information that will be useful to superintendents, FOIPP consultants and school information technologists.

Another important resource for school boards is the Alberta government's *Freedom of Information and Protection of Privacy Policy Guide*, which is available from the Information Management and Privacy Branch of Alberta Labour. This *Policy Guide* outlines the basic principles and legal implications of the *FOIPP Act*.

The following pages provide an overview of key issues and a summary of suggested strategies for school boards with regard to FOIPP and technology. Statements made here do not carry any legal authority. 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

TABLE OF CONTENTS

INTRODUCTION

Alberta's *Freedom of Information and Protection of Privacy Act* (*FOIPP*) supports basic principles that school boards have always upheld—the principles of openness, accountability and transparency. School boards, like other public agencies, recognize the importance of providing access to public information, provided that the release of such information does not infringe on individuals' rights to privacy.

School boards in Alberta participate extensively in communications activities that keep students, parents, employees and the public well informed about the education system and specific school board policies and programs. For example, parents and taxpayers have a right to know how funds for education are being spent, how students are assessed and disciplined, and what results the schools are achieving.

Boards also have policies on the handling of records containing personal information. For example, people have a right of access to personal information records about themselves and a right to correct information that is contained in those records. People also have a right to expect that personal information remains private and confidential, that only appropriate personal information is collected, and that such information is used appropriately.

In other words, the new FOIPP legislation is not introducing radically new concepts or practices. It is, however, using legal "teeth" to require public bodies to be open and accountable, and to enforce stringent protection of privacy. Under FOIPP, all information in the ***control*** or ***custody*** will be considered a ***record*** for the purposes of the *FOIPP Act* and can therefore be the subject of a FOIPP request. (See definitions of bold italicized words in Appendix B, "Definitions.")

The current rapid increase in the use of information technology (computer databases, e-mail, faxes, etc.) is adding an additional variable to the freedom of information/privacy equation. Technology makes it easier to collect and release (or provide access to) large amounts of information. Many people are understandably nervous about technology's potential for invading their privacy and having their personal information accessed for inappropriate uses.

The major solution to this new technological challenge is the use of proper security measures. Consequently, policy and strategies for controlling access to computer databases and e-mail messages are key components of Alberta Education's FOIPP and technology best practices report (*FOIPP and Technology: Best Practices For Alberta School Jurisdictions*, 1999—hereinafter called "the in-depth study").

Records management is another important issue that is becoming even more critical with the advent of technology. Although the use of computers, e-mail and the Internet is increasing exponentially, many people have yet to master the relatively new concept of maintaining workable electronic filing systems. This aspect of record-keeping must be dealt with from the outset, not only in order to comply with the requirements of the *FOIPP Act* but also to achieve other corporate goals such as efficiency.

The focus of this document, and of the accompanying in-depth study, is on policy concerns related to managing and disseminating information, and keeping it secure.

ACCESSING GENERAL INFORMATION

If a school board's communications and data management policies respect the spirit of the *FOIPP Act*, and are effective and efficient, staff can normally expect to deal with a minimal number of formal requests to release information. This is important because handling formal FOIPP requests can be time-consuming and expensive. Often, a confrontational mood develops as well. Ideally, therefore, FOIPP requests should be the avenue of last resort.

Most school boards currently have policies that permit access to certain types of records on request (routine disclosure) and the periodical release of information and/or records (active dissemination). Most boards also have safeguards to ensure that private information remains private and is not distributed inappropriately.

Example of routine disclosure: A board establishes an Internet website where parents and members of the general public can obtain information about results on achievement tests and diploma examinations and/or policies on student conduct. The board also makes the same information available in other formats, on request. The board also provides manuals, guidelines and handbooks to interested citizens on request. Where necessary or desirable, the board charges fees to cover the cost of providing the requested information.

Example of active dissemination: A board issues an annual report that contains a budget and workplan, as well as regular news releases about proposed expenditures on building new schools and/or modernizing older facilities. The board's policy is to report on all topics that the public and the media wish to know about, provided that there is not an issue of privacy involved.

In some cases, disclosure and/or dissemination are required by law. Section 59 of the *School Act* refers to items available on a regular basis, such as minutes of any public meeting or school board meeting, agendas of any public meeting or board meeting, and any other information deemed useful to the public; for example, expense accounts. Usually no exceptions apply to these legal requirements, as sensitive components can often be omitted without much difficulty.

To facilitate communications, many boards now use information technology (Internet websites, e-mail and fax services, reference databases that answer frequently asked questions, other database services, etc.). To ensure access for people who do not have computers, boards may want to consider arranging for access to computers at public libraries and other similar facilities, and providing mail and telephone service as an alternative.

One major effect of the new FOIPP legislation on school boards likely will be a careful review of current practices and policies to determine whether they need to be modified to meet legal requirements. Frequently, past practices will continue to be valid, but there will be some exceptions. A review of the types of inquiries a board receives also would be helpful in determining whether adequate access to general information is being provided. Another issue that will have to be addressed is, "Who has the authority to release which type of information?"

The in-depth study recommends these practices:

- preparing an inventory of current information holdings that includes an assessment of their status (re routine disclosure and active dissemination);

- setting up a co-ordinating committee (particularly in large or decentralized jurisdictions) to develop a corporate approach to routine disclosure and active dissemination and to help implement related practices;
- reviewing past and current inquiries, with a view to minimizing the number of FOIPP requests;
- delegating authority for routine disclosure and active dissemination of information, in order to ensure the rapid and effective release of information.

SUGGESTED STRATEGIES

➢ Maintain and strengthen current communications programs and seek to expand them—both in a spirit of openness, accountability and transparency, and to reduce the number of formal FOIPP requests.

The board should be involved in a variety of communications activities, including routine access and active dissemination.

➢ Develop or review and update an information access policy for the jurisdiction.

The information access policy should be designed to:

- encourage a pro-active approach to information dissemination and access; and
- reflect any requirements arising from the new FOIPP legislation, including protection of privacy.

Development and maintenance of this policy should involve the joint efforts of the FOIPP co-ordinator, interested staff, the communications office and information technologists. In order to keep the policy current, staff should be required to consult with the FOIPP co-ordinator whenever new information systems are created.

➢ Use information technology and electronic media as extensively as possible to make information easily accessible while at the same time providing people who do not have access to computers with alternative sources of the same information.

The other side of this suggestion, of course, is ensuring that technical safeguards are in place so that the public has restricted access to the jurisdiction's electronic records.

ACCESSING PERSONAL INFORMATION AND PROTECTING PERSONAL PRIVACY

Under the *FOIPP Act*, individuals continue to have certain rights of access to ***personal information*** about themselves that is kept on file in a school board's records; for example, information about students, parents, guardians, contact persons, teachers, employees and contracted staff. Since this principle has generally been respected in the past, previous board policies will likely serve, with some modification.

When there is a high demand for a particular type of record, technology can help to make the application process more routine. Adequate authentication procedures will be needed, however, to ensure that applicants for information are who they say they are. Other security features such as encryption also are required to protect the privacy of individuals while still allowing appropriate access.

Privacy issues related to FOIPP may cause school jurisdictions to modify their policies on:

- the collection and compilation of records containing personal information;
- the completeness and accuracy of personal information in records;
- the protection, use, disclosure and retention of personal information.

As with access to general information, it may be necessary and/or desirable to charge a fee to cover the costs of providing certain types of personal information. For example, it is not unusual for educational agencies to charge a fee for copies of student transcripts.

Note: The collection, use and management of student records—as defined in the *School Act* (Section 18) —is a legal process outside of the *FOIPP Act*. Other classes of records that are not covered by the *FOIPP Act* include questions to be used on examinations or tests and records of elected school officials that are not in the control or custody of the school jurisdiction.

Data matching, which includes ***data linkage*** and ***data profiling***, involves the comparison of personal data obtained from different sources for the purpose of making decisions about the individuals to whom the data pertains. Although data matching increases efficiency, it also has the potential to invade the privacy of individuals. Therefore, this is another area that requires a review to ensure compliance with FOIPP legislation. The FOIPP co-ordinator should review all existing and new data matching systems.

New or modified information systems used to collect, compile, process, store, use, disclose or manipulate personal information must reflect the requirements of the *FOIPP Act*. A good method of ensuring FOIPP compliance in these systems is to do a formal privacy impact assessment (PIA) (see Appendix C).

The PIA helps to clarify:

- authority for collection;
- the nature of the information to be collected and the reason for collecting it;
- methods/manner of collection;
- how individuals will be notified of the authority for collection, the purpose of collecting the information and accountability for the collection;

- how accuracy and currency will be maintained;
- how the information will be used, and how usage will be audited;
- what controls will apply to disclosure;
- how data matching and linkage will be handled;
- how security will be maintained;
- how files and records will be managed—both in terms of protecting privacy and maintaining efficiency;
- what impact the proposed record system is likely to have on an individual's right to privacy.

A PIA is best carried out when the system is being designed.

SUGGESTED STRATEGIES

➢ In accordance with the requirements of the *FOIPP Act*, continue to:

- provide individuals with access to information about themselves that is held in school jurisdiction records;
- make corrections as required; and
- keep this private information secure from inappropriate use.

Normally, applicants for personal information would receive the same information through this routine process as they would through an application under the *FOIPP Act*. If this is not the case, the applicant should be so advised.

➢ Develop or review and update the board's policy and procedures on privacy protection.

These policies and procedures should address:

- methods of protecting privacy and keeping records secure in new or modified personal information systems;
- reviewing personal systems, including forms used to collect personal information, to ensure compliance with the *FOIPP Act*;
- security issues;
- data matching issues.

The board's policy on the protection of privacy should require the use of a privacy impact assessment whenever new information systems are introduced or existing systems modified.

➢ To ensure FOIPP compliance, review new and/or modified information systems used to collect, compile, process, store, use, disclose or manipulate personal information.

Boards may wish to seek advice about such a review from the Office of the Information and Privacy Commissioner.

FOIPP AND INFORMATION MANAGEMENT

For a detailed description of issues and strategies related to FOIPP and information management, see Part 6 of the in-depth study.

MANAGING RECORDS

School boards must effectively provide public access to certain types of information while still protecting the privacy of individuals. To achieve these goals, boards need to establish solid information management practices.

Specifically:

1. *Staff must be able to find records; that is, to identify, locate and produce them.*

   Many organizations face great challenges in this area. Searching for records can take up an inordinate amount of time and energy. As well, under the *FOIPP Act*, public agencies are expected to be able to produce various types of records on request. If they can not do this, there may be questions about the adequacy of the search.

2. *There must be assurance that records are complete and accurate.*

   Boards should have standards for documentation, including clear policy on methods of documenting the board's business activities and transactions. Employees must understand the policy and procedures and be held accountable for their actions.

   E-mail and voice mail communications, as well as other technology systems, are raising new questions about which transactions are or are not transitory. For example, electronic documents are now frequently used to support a decision or action of the board, and consequently these documents must be kept in the records. Destroying these documents can be a very serious matter, especially if there is any question of people having done so in order to evade a FOIPP request.

3. *There must be a workable authorized system for destroying/disposing of records.*

   Boards need a process for disposing of records that are inactive and no longer needed for business purposes or the long-term operations of an organization (this is called records scheduling) so they know what records have been destroyed and do not waste time searching for records that do not exist. This process also provides clear direction to staff about which records may be destroyed and when.

   There also should be an archiving system for older records that are not destroyed (those that record the activities of the organization and provide a corporate memory).

4. *There must be an ability to routinely disclose records outside of the FOIPP process while also keeping personal information private.*

As mentioned in the section on "Accessing General Information," making effective decisions about communication and information dissemination can greatly reduce the number of FOIPP requests a board has to deal with.

To achieve all of the above goals, boards need a policy on managing corporate information that addresses the following issues:

- providing direction about the management of **all** records;
- making recorded information a "corporate resource," not the separate domains of individuals, units or schools;
- adopting a life-cycle management approach (direction covering all phases of a record's development: planning, collection or creation, distribution, retrieval, use, transmission, storage, maintenance, protection, disposition and so on);
- assigning accountability for the management of recorded information.

Board policy on information management may include a variety of directives, as follows.

- a directive on managing a record throughout its life cycle;
- a directive for establishing and maintaining record-keeping systems;
- a directive on organizing and filing electronic records;
- a directive on establishing and maintaining a corporate inventory;
- a directive governing the creation and generation of records (document standards);
- a directive on standards for transitory records;
- a directive on the organization, retrieval and storage of records;
- a directive on planning information systems (routine access, active dissemination, protection of privacy);
- a directive on the disposition of records;
- a directive on information management when contractors are involved.

SECURITY

Security has always been a major concern in information management, but this issue has become even more significant now that technology is being used extensively. Consequently, boards need to develop or review and update a policy on security that includes expectations of staff, a method for auditing the adequacy of current security techniques and a method for assessing threats and risks (see Appendix D, Security Summary Table, and Appendix E, Evaluating Network Security).

Effective security involves much more than locking up records and throwing away the key. The secured records must still be accessible as needed (availability), sensitive information must not be disclosed inappropriately (confidentiality) and the records must be accurate and complete (integrity).

Examples of administrative, physical and technical safeguards required for information technology include:

- written staff responsibilities and security procedures;
- strategies for dealing with the loss of computer-based data or capabilities;
- physical barriers, security zones, access and authorization mechanisms and locked containers to restrict access;
- proper containers and procedures for the secure processing, storage, transmission and disposal of information and other assets;
- access controls on software, hardware and operating systems;
- secure communications and cryptography where warranted.

E-MAIL

E-mail has raised a whole set of new questions and issues, including decisions about destroying messages, the protection of privacy (what is and is not an appropriate subject for an e-mail message) and the surreptitious monitoring of personal e-mail. Many people do not realize that e-mail communications within a public body are records and can therefore be the subject of a FOIPP request.

This topic is addressed in detail in Part 6 of the in-depth study.

SUGGESTED STRATEGIES

- Develop a FOIPP-compliant policy on managing corporate information, including the management of electronic records.
- Develop a FOIPP-compliant policy on security of information for all records kept by the school board, including electronic records.

  The policy should address the accountability of staff and management, and provide for an audit mechanism. An excellent way of achieving security is to use a life-cycle management approach.
- Develop a FOIPP-compliant policy on the use and management of e-mail.

APPENDIX A
SUMMARY OF SUGGESTED SCHOOL BOARD STRATEGIES

- Maintain and strengthen current communications programs and seek to expand them—both in a spirit of openness, accountability and transparency, and to reduce the number of formal FOIPP requests.

- Develop or review and update an information access policy for the jurisdiction.

- Use information technology and electronic media as extensively as possible to make information easily accessible while at the same time providing people who do not have access to computers with alternative sources of the same information.

- In accordance with the requirements of the *FOIPP Act*, continue to:
  - provide individuals with access to information about themselves that is held in school jurisdiction records;
  - make corrections as required; and
  - keep this private information secure from inappropriate use.

- Develop or review and update the board's policy and procedures on privacy protection.

- To ensure FOIPP compliance, review new and/or modified information systems used to collect, compile, process, store, use, disclose or manipulate personal information.

- Develop a FOIPP-compliant policy on managing corporate information, including the management of electronic records.

- Develop a FOIPP-compliant policy on security of information for all records kept by the school board, including electronic records.

- Develop a FOIPP-compliant policy on the use and management of e-mail.

APPENDIX B
DEFINITIONS

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

Control of a record. The school jurisdiction has the authority to manage, restrict, regulate or administer the use, disclosure, and disposition of the record. As an example, a record may be in the *custody* of a contractor but still in the *control* of the school jurisdiction.

Data linkage. See "data matching."

Data matching. The comparison of personal data obtained from different sources (both electronic and paper formats) for the purpose of making decisions about the individuals to whom the data pertains. Data matching therefore involves the collection, use and disclosure of personal information. Included in the definition of data matching is data linkage, also known as data profiling.

Data profiling. See "data matching."

Personal information. Recorded information about an identifiable individual; for example, name, address, date of birth, age, sex, religion, blood type, opinions. Personal information also includes other people's opinions about the individual.

Record. A record may take many forms, including electronic documents and electronic messages and notes, as well as draft materials created in carrying out school jurisdiction business. Software and/or any mechanisms that produce records are not included in the definition of a "record." A FOIPP request may deal only with records.

APPENDIX C
PRIVACY IMPACT ASSESSMENT
(Excerpted from FOIPP and Technology: Best Practices For Alberta School Jurisdictions)

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.

APPENDIX D
SECURITY SUMMARY TABLE
(Excerpted from FOIPP and Technology: Best Practices For Alberta School Jurisdictions)

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

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

APPENDIX E
EVALUATING NETWORK SECURITY
(Excerpted from FOIPP and Technology: Best Practices For Alberta School Jurisdictions)

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

APPENDIX F
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: 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).

U.S. Department of Education
Office of Educational Research and Improvement (OERI)
National Library of Education (NLE)
Educational Resources Information Center (ERIC)

NOTICE

REPRODUCTION BASIS

☒ This document is covered by a signed "Reproduction Release (Blanket) form (on file within the ERIC system), encompassing all or classes of documents from its source organization and, therefore, does not require a "Specific Document" Release form.

☐ This document is Federally-funded, or carries its own permission to reproduce, or is otherwise in the public domain and, therefore, may be reproduced by ERIC without a signed Reproduction Release form (either "Specific Document" or "Blanket").