



Cloud Computing and Privacy Toolkit

Protecting Privacy Online

May 2016

Alberta ■
Government

Table of Contents

- ABOUT THIS TOOLKIT 4**
 - What is this Toolkit? 4
 - Purpose of this Toolkit..... 4
 - Intended Audience 5
 - Legal Disclaimer 5

- KEY DEFINITIONS 6**

- INTRODUCTION 7**
 - Why is Protecting Privacy Important? 7
 - Who Needs to Be Involved In Protecting Privacy? 8
 - Sections of Toolkit 8
 - Section 1: Key Concepts 8
 - Section 2: Considerations for Assessing Readiness for Cloud 8
 - Section 3: Protecting Privacy When Selecting Cloud Services 9

- SECTION 1: KEY CONCEPTS..... 11**
 - Managing Use of Cloud Services 11
 - Using Cloud Services Located Outside of Canada 12
 - Managing Privacy Considerations 12
 - Considering Benefits and Risks..... 13
 - Adapting Governance and Decision Making Approach..... 13
 - Reducing the Impact on Privacy 14

- SECTION 2: CONSIDERATIONS FOR ASSESSING READINESS FOR CLOUD 16**
 - Getting Started 17
 - Step 1: Obtain Senior Management Commitment and Support..... 17
 - Step 2: Identify Personal Information 17
 - Step 3: Conduct a Risk Assessment 18
 - Step 4: Design/Implement Privacy Controls..... 19
 - Step 4.1: Define Roles and Responsibilities 19
 - Step 4.2: Create or Update Policies, Administrative Procedures and Guidelines..... 19
 - Step 4.3: Utilize Risk Assessment Tools..... 20
 - Step 4.4: Raise Awareness and Provide Professional Development..... 21
 - Step 4.5: Adapt Breach and Incident Management Response Processes..... 21
 - Step 4.6: Manage Cloud Service Providers..... 21
 - Step 4.7: Communicate and Demonstrate Accountability..... 22
 - Step 5: Monitor Effectiveness of Controls..... 22



SECTION 3: PROTECTING PRIVACY WHEN SELECTING CLOUD SERVICES	25
Overview of Process	25
Protecting Privacy When Selecting Cloud Services Flowchart	27
Step 1: Determine Desired Results.....	30
Step 2: Is Personal Information Involved?.....	30
Step 3: Monitor Personal Information	30
Step 4: Evaluate Benefits, Costs and Risks of Cloud Services.....	31
Step 5: Determine Who Needs to be Involved.....	32
Step 6: Assess Service Options	32
Step 7: Is a Privacy Impact Assessment (PIA) Advisable?.....	32
Step 8: Assess Privacy Requirements	33
Step 9: Communicate Requirements and Consider Response	34
Step 10: Re-evaluate Rationale and Risks	34
Step 11: Select Preferred Service Provider.....	35
Step 12: Determine Contract.....	36
Step 13: Are Residual Risks Acceptable?	36
Step 14: If Residual Risks are Acceptable, Formalize Contract.....	36
Step 15: If Residual Risks are not Acceptable, Reconsider Goals & Options.....	36
Appendix A: Glossary	37
Appendix B: Cloud Computing Evolution and Benefits	40
Appendix C: How Does Use of Cloud Services Impact Privacy?	41
Appendix D: Privacy Legislation Considerations	44
What Legislation Applies and to Whom?	44
Is Storing or Accessing Personal Information Outside of Canada Allowed?	45
Is Complying with the FOIP Act Enough?	45
Appendix E: Key Challenges of Managing Cloud Privacy Risks	46
Appendix F: Risk Management Considerations and Approaches	47
Appendix G: Streamlining Cloud Service Selection/Approval Processes	49
Appendix H: Assessing Residual Risk	50
Appendix I: Additional Resources	53



ABOUT THIS TOOLKIT

WHAT IS THIS TOOLKIT?

This toolkit contains practical tools and resources for ensuring the protection of privacy when selecting and using cloud services. Toolkit components include:

- key concepts for protecting privacy in the cloud, such as why the topic is important, how cloud services impact privacy and privacy legislation considerations;
- considerations for assessing school authority readiness for cloud and implementing or updating privacy safeguards; and
- additional resources including guidance for managing privacy risks when selecting cloud services.

PURPOSE OF THIS TOOLKIT

This toolkit was developed to:

- raise awareness of the privacy risks associated with use of cloud services;
- provide practical tools and resources for making decisions involving protection of privacy in the cloud; and
- assist with protecting privacy while enabling innovative use of cloud services for learning and administration.

The resources are tailored for the education context to assist school authorities in identifying and mitigating privacy risks when considering cloud services, without unduly delaying or complicating decisions related to such services.

This toolkit applies to cloud services the school authority directly contracts and manages. The toolkit does not apply to agreements between individual school authority leaders and cloud providers, such as when instructional leaders personally register for cloud services for use in learning environments.

School authorities are advised to develop administrative policies that govern staff members' personal use of cloud services for instructional use.



INTENDED AUDIENCE

This toolkit was developed in consultation with Kindergarten to Grade 12 (K-12) education leaders from across Alberta.

It was developed for the following key stakeholder groups at Alberta public, separate and charter school authorities subject to Alberta's *Freedom of Information and Protection of Privacy Act* (FOIP Act), including:

- Superintendents
- Secretary-Treasurers
- Technology leaders
 - Educational Technology (ET) leaders
 - Information Technology (IT) leaders
- FOIP co-ordinators.

School administrators, instructional leaders, support staff and other stakeholders may also find this toolkit relevant.

Much of this toolkit can be used by organizations that are subject to other privacy legislation such as private school authorities subject to the *Personal Information Protection Act* (PIPA). However, some adjustments may be required. These organizations are advised to consult their legal counsel and/or privacy officers before acting.

This toolkit is not prescriptive. Each school authority has unique needs, history and culture to consider when making decisions about protecting privacy with cloud services. Adapt guidance to your context and make use of the additional tools and resources as needed.

LEGAL DISCLAIMER

This toolkit does not represent legal advice or acceptance of liability on the part of the Government of Alberta. It is for information purposes only and is intended to provide supporting resources and practical information as a starting point for making decisions about cloud computing and privacy. As always, readers should ensure they have sought professional legal advisement and consulted their *Freedom of Information and Protection of Privacy Act* (FOIP Act) co-ordinators on all policy and legislative compliance related matters. This guidance may be inappropriate in some respects for private school authorities subject to the *Personal Information Protection Act* (PIPA).



KEY DEFINITIONS

Below are definitions of some key terms related to protecting privacy in the cloud.

Cloud computing is a model for network or Internet access to shared resources, software and information. It is delivered as a service that computers or mobile devices can access on demand. Examples of cloud services include Google Apps for Education, YouTube, Skype, Blackboard and other popular websites and online services. See the [Cloud Computing Tech Briefing](#)¹ for more information.

Privacy involves individuals' rights to control the collection, use and sharing of their personal information with others. Privacy is a fundamental human right that is a cornerstone of other freedoms in our society. It encompasses a number of aspects including physical, communication, behavioural and information privacy.

Personal information is any information about an identifiable individual, including identifiers (name, Alberta Student Number, social insurance number, etc.), characteristics (birth date, gender, address, etc.) and personal history (education, job history, medical records, etc.), as well as any other information associated with an identifiable individual. The [FOIP Act](#) contains a definition of [personal information](#) that assists public bodies in determining what personal information they need to protect under the Act.

Privacy breach: a privacy breach occurs when there is unauthorized collection, use or access to personal information.²

¹ Alberta Education. (2013, May 1). *Cloud Computing Tech Briefing*. Retrieved from the Alberta Education website: <https://education.alberta.ca/media/3114992/cloud-computing-tech-briefing.pdf>

² Office of the Information and Privacy Commissioner (OIPC). (2015, May). *Key Steps in Responding to Privacy Breaches*. Retrieved from the Alberta Office of the Information and Privacy Commissioner website: https://www.oipc.ab.ca/media/652724/breach_key_steps_responding_to_breaches_jul2012.pdf



INTRODUCTION

[Cloud computing](#) offers school authorities many compelling opportunities to enhance learning, instruction and administration of education. A wide variety of online services and shared computing resources are managed and delivered through cloud computing.

Cloud computing is already used extensively in education.³ Learners, educators and administrators use free or low-cost cloud-based services on a daily basis. Cloud services support personalized learning, social interaction, content creation, publishing, collaboration and administration of education. Examples of cloud services include Google Apps for Education, YouTube, Skype and Office 365.

WHY IS PROTECTING PRIVACY IMPORTANT?

While cloud computing has many [benefits](#), it also involves risks, and has privacy and security implications that need to be managed. Protecting privacy in the cloud is a critical issue for K-12 school authorities in Alberta for the following reasons:

- **School authorities are accountable for complying with Alberta privacy legislation** and protecting the privacy of personal student and staff information, including personal information that is stored in the cloud. Under the FOIP Act, you cannot delegate the responsibility for complying with privacy legislation to a cloud service provider, although you may require the provider to take actions to satisfy your responsibility.

See [Appendix D: Privacy Legislation Considerations](#) for more information.

- **A [privacy breach](#) can have serious consequences for students, staff members and your school authority.** Consequences can include increased risk to student/staff safety (if sensitive personal information is exposed that could be used to harm students or staff), potential harm to school authority reputation and exposure to legal action or risk of non-compliance with privacy legislation.
- **As the use of cloud services to facilitate student-centred learning and efficient administration increases, the importance of protecting privacy in the cloud grows.**

*Policy Direction 5 of Alberta Education's [Learning and Technology Policy Framework](#) recommends that school authorities provide students, teachers, administrators and other educational professionals with access to reliable infrastructure, high-speed networks and digital learning environments in order to support student-centred learning with technology. This requires that school authorities **ensure the administration of safe and secure technologies**, and adopt and maintain effective practices for information technology (IT) governance, IT management and information security management.*

³ New Media Consortium. (2014). *NMC Horizon Report: 2014 K-12 edition*. Pg. 36. Retrieved from <http://cdn.nmc.org/media/2014-nmc-horizon-report-k12-EN.pdf>



Protecting the privacy of personal student and staff information is a critical component of providing safe and secure technologies as recommended in Policy Direction 5.

See [Learning and Technology Policy Framework](#)⁴ for more information.

WHO NEEDS TO BE INVOLVED IN PROTECTING PRIVACY?

School authority leaders, educators, technology leaders, legal counsel and FOIP co-ordinators have an important role to play in ensuring that privacy is protected when making decisions about cloud-based services.

See [Step 4.1: Define Roles and Responsibilities](#) of Section 2 for more information.

SECTIONS OF TOOLKIT

To assist school authority decision makers with managing privacy risks for cloud services, this toolkit covers the information below:

Section 1: Key Concepts

This section covers some key concepts that are important for school authority decision makers to understand about protecting privacy in the cloud.

See [Section 1: Key Concepts](#) for more information.

Section 2: Considerations for Assessing Readiness for Cloud

This section discusses considerations for assessing school authority readiness for cloud and for implementing appropriate privacy safeguards.

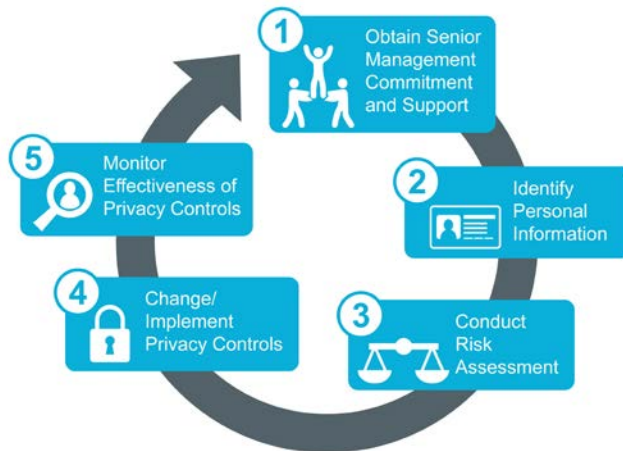


Figure 1: Considerations for Assessing Readiness for Protecting Privacy in the Cloud

See [Section 2: Considerations for Assessing Readiness for Cloud](#) for more information.

⁴ Alberta Ministry of Education. (2013). *Learning and Technology Policy Framework (LTPF)*. Pg. 39-40. Retrieved from the Alberta Education website: <https://education.alberta.ca/media/1046/learning-and-technology-policy-framework-web.pdf>

Section 3: Protecting Privacy When Selecting Cloud Services

This section includes guidance for managing privacy risks when selecting individual cloud services. It provides a high-level summary of steps school authorities might use when analyzing needs, considering privacy and selecting cloud computing services for learning and administration.

This section is best suited for selecting cloud services involving substantial privacy risks such as storage of highly sensitive personal information and/or services used throughout the school authority by a significant number of staff or students.

Consider these guiding questions when making decisions about a particular cloud service:

- 1. What outcomes are we trying to achieve?**
- 2. Is personal information involved?**
- 3. What are our options for achieving our outcomes? Consider available cloud services, local or hosted technology services and other possible approaches.**
- 4. Who needs to be involved in making the decision?**
- 5. How are we going to evaluate our options, i.e., what is our evaluation criteria?**
- 6. How will we assess and manage privacy risks?**
- 7. What process will we follow to ensure that privacy risks are managed appropriately?**

See [Section 3: Protecting Privacy When Selecting Cloud Services](#) for more information.



SECTION 1: KEY CONCEPTS



SECTION 1: KEY CONCEPTS

This section covers some key concepts that are important for school authority decision makers to understand when protecting privacy in the cloud.

MANAGING USE OF CLOUD SERVICES

Cloud services pose a number of challenges to ensuring effective governance, risk management and compliance with privacy legislation. Some of the key challenges include:

- **Difficulty managing adoption of services:** Many cloud services are free or low cost, allowing anyone to sign up for cloud services in a matter of minutes. Organizational procurement, approval and due diligence processes can easily be bypassed, exposing the organization to significant risk.
- **Underestimating the level of risk:** Due to the low cost and effort involved in setting up the cloud service, senior leaders may underestimate the magnitude of the risk involved in putting sensitive personal information in the cloud. For example, a behaviour management app that allows instructional leaders to recognize and reinforce student behaviour in real time using a smartphone or tablet requires the storage of student names, parent emails and student behaviours. It may be free or easy to set up, yet involve significant risk due to the sensitivity of the personal information.
- **Lack of transparency:** Staff and students may not know when information is in the cloud versus on a local device. For example, some laptops store most of their data directly in the cloud. Apps on smart phones often store data or backup data to the cloud. Sensitive personal information may inadvertently be stored in the cloud because people are not aware of where the information is actually located.

Lack of awareness and understanding can result in acceptance of significant privacy risks without understanding the implications.

See [Appendix E: Key challenges of Managing Cloud Privacy Risks](#) for more information.

The above challenges can be addressed by adopting a systematic approach to protecting privacy in your organization.

See [Section 2: Considerations for Assessing Readiness for Cloud](#) for more information.



USING CLOUD SERVICES LOCATED OUTSIDE OF CANADA

Privacy legislation does not prohibit school authorities from using cloud service providers that are located outside of Canada. However, it can be more difficult to ensure compliance with privacy legislation, as these service providers are not subject to Canadian privacy laws.

Such issues can often be managed, especially if service providers are willing to negotiate contract terms, but they require careful attention to privacy and security compliance obligations to ensure that equivalent privacy protections are specified in the contract. While a service provider may follow strong security practices, security is not the same as privacy. Your school authority is still accountable for ensuring adequate protection of personal information under privacy legislation obligations and cannot delegate that accountability to a service provider. Consult your FOIP co-ordinator and legal counsel for more information.

See [Appendix D: Privacy Legislation Considerations](#) for more information.

MANAGING PRIVACY CONSIDERATIONS

Managing privacy considerations for cloud services is significantly different than for traditional outsourced or locally hosted services. Many cloud service providers base their business models on economies of scale. They often require acceptance of standard contracts and are not willing to negotiate their terms of service. These standard contracts may not ensure compliance with privacy legislation or provide remedies if there are breaches. Nevertheless, school authorities cannot contract out of their legislated privacy obligations. They are still accountable for protecting the privacy of personal student and staff information that has been transferred to cloud service providers.

If contract terms are not negotiable, procuring cloud services then involves comparing available options and selecting the best choice (or not storing personal information in the cloud if the personal information is sensitive and the risk is too great).

See [Appendix C: How Does Use of Cloud Services Impact Privacy?](#) for more information.



CONSIDERING BENEFITS AND RISKS

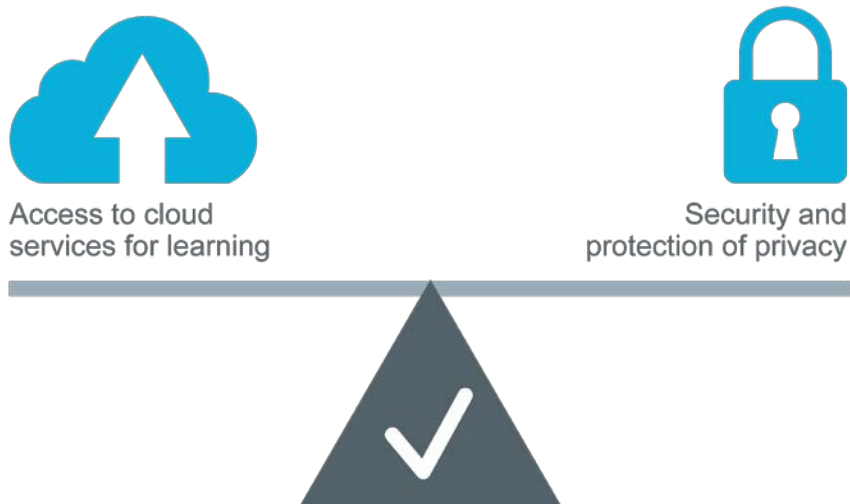


Figure 2: Consider Benefits and Risks

Privacy is an important consideration that cannot be ignored. However, it is not possible to eliminate all privacy risks. Appropriate planning considers the benefits, costs and management of risks. This is critical to enable the innovative use of cloud services for learning or administration and to ensure compliance with privacy legislation.

See [Section 3: Protecting Privacy When Selecting Cloud Services](#) for more information.

ADAPTING GOVERNANCE AND DECISION MAKING APPROACH

Consider adapting the level of privacy risk management and governance applied to individual cloud services to be proportional to the sensitivity of the personal information involved and the degree of risk.

For example, services such as Student Information Systems (SIS) contain substantial amounts of sensitive personal information and are used by a large number of people for critical work on a regular basis. When making decisions about these types of services, it is necessary to engage in detailed planning, thorough risk management and broad consultation. Other types of services, such as a blog or a specific learning resource tend to be used by fewer people, and the information in them tends to be less sensitive. Decisions about these systems could be delegated to instructional leaders, provided they have the guidance and skills required to evaluate the potential privacy risks of the information they are working with.

If personal information is involved, the [FOIP Act](#) applies. Some types of personal information may not be suitable for storing in the cloud due to their sensitivity or value and the level of risk involved.

See [Step 4: Evaluate Benefits, Costs and Risks of Cloud Services](#) of Section 3 for factors to consider when determining the rigour of planning, risk management and consultation needed to adequately address privacy risks.

REDUCING THE IMPACT ON PRIVACY

The impact on privacy is greatly reduced if little or no personal information is sent to the cloud. Where possible, it is always preferable to minimize the amount of personally identifiable information sent to the cloud.

While public bodies such as school authorities are required to comply with the FOIP Act at all times, FOIP security requirements are broadly stated and allow for flexibility in the management of security risk. For example, while the FOIP Act does not distinguish between the sensitivity of different kinds of personal information, it is entirely consistent with FOIP to do so when implementing information security measures. There is room to consider more or less secure approaches to the protection of personal information, as long as the selected approach is appropriate for the sensitivity of the information needing protection. Such risk management alternatives may provide more choice in the selection of cloud service providers, especially if it is possible to reduce the amount or sensitivity of personal information that is involved.

Privacy scans and Privacy Impact Assessments can assist with assessing and managing privacy risks. They are highly recommended by Alberta's Information and Privacy Commissioner.

See [Appendix F: Risk Management Considerations and Approaches](#) for more information.



SECTION 2: CONSIDERATIONS FOR ASSESSING READINESS FOR CLOUD



SECTION 2: CONSIDERATIONS FOR ASSESSING READINESS FOR CLOUD

Consider assessing school authority readiness for protecting privacy in the cloud and, if needed, implementing a comprehensive approach to protecting privacy that integrates cloud privacy considerations with your school authority's privacy program. The following process for building an effective privacy program⁵ can be adapted for protecting privacy in the cloud.

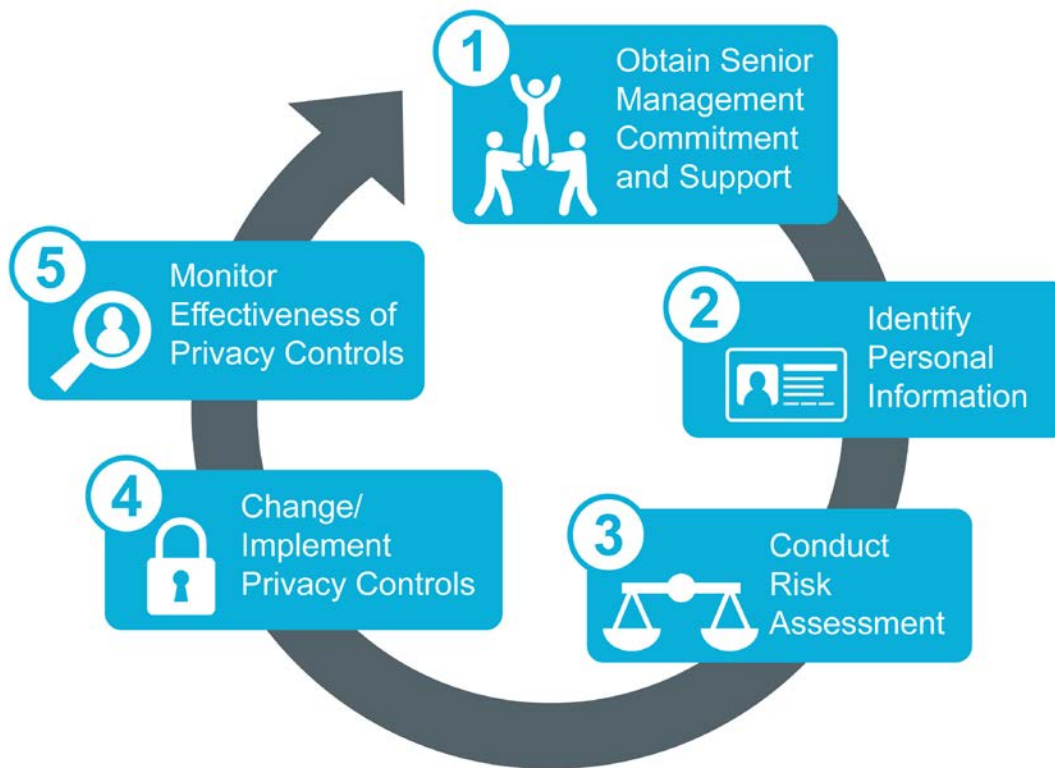


Figure 3: Considerations for Assessing School Authority Readiness for Protecting Privacy in the Cloud

⁵ Section 2 has been adapted from guidance prepared by the Office of the Information and Privacy Commissioner for British Columbia and for Alberta and the Office of the Privacy Commissioner of Canada:

- Office of the Privacy Commissioner of Canada. (2012, April 17). *Getting Privacy Right with a Privacy Management Program*. Retrieved from the Office of the Privacy Commissioner of Canada website: https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp
- Office of the Information and Privacy Commissioner for British Columbia. *Accountable Privacy Management in BC's Public Sector*. Retrieved from the Office of the Information and Privacy Commissioner for British Columbia Website: <https://www.oipc.bc.ca/guidance-documents/1545>

GETTING STARTED

If your organization does not yet have a plan in place to protect privacy in the cloud, consider initiating a project. Designate a project leader and team members to integrate cloud services privacy management into your privacy program.

It is important to monitor and evaluate progress throughout to ensure that the project stays on track and achieves intended outcomes.

STEP 1: OBTAIN SENIOR MANAGEMENT COMMITMENT AND SUPPORT



In most school authorities, the superintendent is ultimately accountable for complying with privacy legislation.⁶ It is important for the superintendent and senior leaders to understand the privacy implications of cloud services and demonstrate strong commitment and support for protecting privacy when selecting cloud services. They should be involved in decision making related to cloud service deployments for the school authority including providing the necessary resources. They should also be aware of any privacy implications that may arise from such deployments and should consult with their FOIP co-ordinator and/or legal counsel as necessary.

STEP 2: IDENTIFY PERSONAL INFORMATION



Consider identifying the types of personal information, especially sensitive information, that is or will be stored in the cloud. Regardless of how mature your school authority's cloud privacy management is, all school authorities can benefit from carefully examining the personal information being held in the cloud and assessing how it's being protected. It may be worth re-examining the purpose for collecting the information to determine if it still needs to be collected.

Key questions to consider include:

- **What personal information is collected and stored in the cloud?**
- **What is the nature and sensitivity of the personal information? This includes any new personal information collected by cloud service providers when using the service.**

The sensitivity of the personal information that is or will be provided to the cloud service provider is of particular importance. In certain circumstances, disclosure of even apparently innocuous personal information could have detrimental consequences for a student or staff member if disclosed to the wrong parties. As much as possible, minimize the amount of personal information transferred to the cloud.

⁶ A Board resolution assigning responsibility for FOIP decisions to specific persons should be on record. This responsibility is usually assigned to the superintendent, or a combination of the superintendent and other leaders via a policy sometimes known as a "delegation matrix."

In some cases, the importance of protecting personal information may outweigh the benefits of the cloud service. This can only be determined if it is known in advance what personal information will be involved.

Note: *Personal information about any student with disclosure restrictions (formerly known as a “protected student”) should not be transferred to cloud services unless a careful risk analysis for that particular student determines that it would not be detrimental. It is important that students with disclosure restrictions are identified before any student information is transferred to the cloud.*

STEP 3: CONDUCT A RISK ASSESSMENT



Consider conducting an overall risk assessment of your school authority’s approach to protecting privacy in the cloud to identify gaps or risks, and rate them to help prioritize which gaps or risks to address first.

Key questions to consider include:

- **Has your school authority defined roles and responsibilities related to managing privacy risks for cloud services? Has it been determined who will be assigned the roles and responsibilities?**
- **Do appropriate administrative procedures, policies and procedures exist that effectively manage privacy risks with cloud-based services? Are procedures or processes in place to manage service providers?**
- **Have appropriate privacy risk assessment tools been identified or developed to assist in assessing the privacy risks of cloud services?**
- **Has your school authority’s breach and incident management response protocols been updated to address cloud-based breaches and incidents?**

After you have identified gaps and overall risks, analyze the risks and identify how you will address them.

Key questions include:

- **What is the potential impact and the probability of the risks occurring?**
- **How will your school authority address the risks?** Possible actions include implementing mitigation measures, transferring the risk to others or accepting the risk, etc.

See [Step 4: Design and Implement Privacy Controls](#) for assistance with answering these questions.



STEP 4: DESIGN AND IMPLEMENT PRIVACY CONTROLS



Privacy controls are the administrative, technical and physical safeguards employed within organizations to mitigate privacy risks. Your organization likely has many of the following privacy controls already in place to manage risk; however, they may just need to be adapted for managing cloud privacy risks if necessary.

Step 4.1: Define Roles and Responsibilities

Making decisions about cloud computing and privacy often involves complex legal, financial, compliance and technical issues. The following people have important roles to play:

- **The head of the organization** (typically the superintendent or the board)⁷ is ultimately accountable for complying with privacy protection requirements under the FOIP Act. Their leadership and understanding of the school authority's operations are fundamental to the successful adoption of cloud services.
- **FOIP co-ordinators** contribute their understanding of the educational implications of the FOIP Act. They are responsible for managing the protection of personal information and often coordinate or lead the development of privacy scans and [Privacy Impact Assessments](#).
- **Legal counsel** for school authorities provide specific legal advice that enable school authorities to effectively make decisions and manage privacy risks.
- **Information Technology (IT) leaders and staff** can provide essential information about both internal and external services. They often play a key role in vetting and selecting cloud services as well as offering information security solutions that can help protect privacy. They may contribute technical expertise in cloud computing and security. Consider consulting experts in these areas if staff do not have this expertise.
- **Educational Technology (ET) leaders** provide essential expertise regarding pedagogy and learning applications for cloud services that will be used in the educational context.
- **Secretary Treasurers or financial leaders** provide expertise and guidance in the areas of budgeting, procurement and contract negotiations.
- **Stakeholders** can provide unique insights regarding the priorities of those impacted by the service – both internal staff members and external groups.

Step 4.2: Create or Update Policies, Administrative Procedures and Guidelines

Cloud computing policies and guidelines may be part of broader policies related to the technology environment, or they may be specific to cloud computing. In either case, the policies and guidelines should clearly identify responsibilities and accountabilities related to cloud computing. For example:

⁷ A Board resolution assigning responsibility for FOIP decisions to specific persons should be on record. This responsibility is usually assigned to the superintendent, or a combination of the superintendent and other leaders via a policy sometimes known as a "delegation matrix".



- Identify who is authorized to enter into cloud service agreements on behalf of the school authority.
- Document what the authorized persons are required to do and the risks they are expected to consider when doing so.
- Consider creating a checklist of considerations to review when making decisions about adopting cloud computing services (see [Section 3: Protecting Privacy When Selecting Cloud Services](#) for some considerations).

Ensure that policies, administrative procedures and guidelines appropriate for assessment, authorization and management of cloud services have been created or updated.

Review school authority privacy and security policies and determine if they are sufficient to support use of cloud services. School authorities may wish to consider guidance provided by the ISO/IEC 27000 series of international information security standards⁸, particularly [ISO/IEC 27002](#)⁹ and [ISO/IEC 27018](#)¹⁰ as they offer sound guidance for the development of information security policies.

Step 4.3: Utilize Risk Assessment Tools

It is important to be aware of privacy risks associated with a cloud service before committing to it. The assessment of such risks may range from cursory to extensive, depending on the nature, sensitivity and volume of personal information involved, the nature and terms of service, the likelihood and severity of a privacy breach, and other factors.

While it is usually not possible to eliminate all privacy risks associated with a cloud service, it is possible to identify those risks that require mitigation in order for the overall level of risk to be within an acceptable level. It is critical to be aware of the remaining risks and to be comfortable that the benefits outweigh those risks.

Privacy scans and impact assessments are a valuable tool for assessing and mitigating the privacy risks of cloud services.

See the following resources for additional information concerning privacy risk assessments:

- [Appendix F: Risk Management Considerations and Approaches](#)
- [FOIP Guidelines and Practices Manual](#)¹¹
This manual provides a large volume of advice and guidance related to FOIP compliance. Privacy Impact Assessments (PIAs) and other privacy matters are discussed in [Chapter 9](#).
- [Privacy Impact Assessment Requirements](#)
The Office of the Information and Protection of Privacy Commissioner (OIPC) in Alberta provides information on privacy impact assessment requirements for achieving compliance with the *Health Information Act*. The OIPC guidance can also be used for FOIP PIAs with minor changes.

⁸ International Standards Organization. *ISO/IEC 27000:2014*. Retrieved from the ISO website: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en>

⁹ International Standards Organization. *ISO/IEC 27002:2013*. Retrieved from the ISO website: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en>

¹⁰ International Standards Organization. *ISO/IEC 27018:2014*. Retrieved from the ISO website: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en>

¹¹ Service Alberta. (2009). *FOIP Guidelines and Practices: 2009 Edition*. Retrieved from the Service Alberta website: <http://www.servicealberta.ca/foip/resources/guidelines-and-practices.cfm>



These requirements provide a comprehensive assessment of privacy risks and mitigation measures.

- [PIA template for local public bodies](#)¹²

This PIA template from Service Alberta is suitable for preliminary PIAs and privacy scans. It addresses matters of FOIP authority, but does not provide a full assessment of privacy risks and mitigation measures.

Step 4.4: Raise Awareness and Provide Professional Development

People need to understand what personal information is, why it needs to be protected and the privacy risks of using cloud services without appropriate due diligence. It is important to help people understand why they sometimes need to trade convenience for privacy and to encourage desirable behaviours.

Ensure that school authority staff members are aware of policies and guidelines related to cloud computing and privacy. Ensure that they have the training and resources to comply with them.

Service Alberta offers [general FOIP training](#)¹³, including training specifically related to FOIP privacy provisions. Training options include instructor-led and online training.

Step 4.5: Adapt Breach and Incident Management Response Processes

Typically, cloud services providers have more responsibilities in the area of breach and incident management response processes than when dealing with internally managed technology services. Ensure that cloud provider capabilities and terms of service include appropriate breach and incident management responses¹⁴. Review school authority breach and incident response processes to ensure they are relevant for breaches occurring in cloud services.

[Breach response guidelines](#)¹⁵ are available from the OIPC.

Step 4.6: Manage Cloud Service Providers

The most important element of managing cloud service providers involves managing the contract with the service provider. A strong contract will mitigate many of the risks that may arise in a cloud computing relationship. Unfortunately, many standard cloud computing service agreements have weak protections for privacy. If possible, negotiate appropriate terms with the service provider.

If the contract terms are not negotiable, procuring cloud services then involves comparing available options and selecting the best choice (or not storing personal information in the cloud if the personal information is sensitive and the risk is too great). See [Section 3: Protecting Privacy When Selecting Cloud Services](#) for more information. Consider involving your FOIP co-ordinator and legal counsel in the development or review of contracts and service agreements.

¹² Service Alberta. *Privacy Impact Assessment Templates*. Retrieved from the Service Alberta website:

<http://www.servicealberta.ca/foip/resources/3540.cfm> (click on the PIA – Local link)

¹³ Information on FOIP Training for Public Bodies is available on the Service Alberta website:

<http://www.servicealberta.ca/foip/training-for-public-bodies.cfm>

¹⁴ Organizations subject to the *Personal Information Protection Act* (PIPA) are required to report privacy breaches. These provisions apply to breaches involving cloud service providers as well as the organization's own systems.

¹⁵ Office of the Information and Privacy Commissioner (OIPC). (2015, May). *Key Steps in Responding to Privacy Breaches*. Retrieved from the Alberta Office of the Information and Privacy Commissioner website:

https://www.oipc.ab.ca/media/652724/breach_key_steps_responding_to_breaches_jul2012.pdf



Some Suggested Contractual Provisions

Retain ownership of personal information
Prevent personal information from being used for other purposes
Ensure the appropriate collection, use and sharing of personal information, in keeping with FOIP requirements
Ensure personal information is deleted appropriately and securely
Ensure provider is liable for privacy/security breaches
Ensure adequate breach identification and response procedures
Include ability to review provider's privacy/security measures and to audit the services provided or gain access to vendor-funded audit reports. ¹⁶

Note: Negotiated cloud service contracts should include provisions to permit the review and/or audit of the provider's services and the investigation of breaches. In the absence of comprehensive audit provisions, it is important for service providers to provide access to the results of third party audits. Most reputable service providers conduct this type of audit on an annual or bi-annual basis.

While such audits may not address all areas of the provider's operations needed for FOIP compliance, they usually highlight major risk areas, especially those related to information security. (Note that such risks will often be mitigated to the provider's satisfaction before any audit report is released.)

If you are willing and able to review or audit the service provider, the [Generally Accepted Privacy Principles](#)¹⁷ (GAPP) provide a suitable privacy audit framework. Although the principles are legislation independent, they are similar to those that underpin the FOIP Act and PIPA.

GAPP is an extensive framework that most school authorities would find onerous to apply in its entirety. However, it is possible to set the scope of the audit to the higher, less detailed levels.

Step 4.7: Communicate and Demonstrate Accountability

While privacy legislation does not require that stakeholders be informed when storing personal information in the cloud, it is still a good practice to inform them.¹⁸ Consider explaining the measures taken to ensure that privacy is protected and that appropriate responses will take place in the event of a breach.

STEP 5: MONITOR EFFECTIVENESS OF CONTROLS



As technology evolves rapidly, new opportunities and privacy risks continue to emerge. Assess the effectiveness of privacy protection measures and adjust as needed on an ongoing basis.

School authorities are advised to conduct periodic reviews of cloud services and related service agreements. How frequently should cloud services be reviewed? It depends on the nature and

¹⁶ Most major cloud service vendors undertake periodic audits of their facilities and services, but they may be reluctant to provide access to the reports of those audits.

¹⁷ American Institute of CPAs. *Generally Accepted Privacy Principles*. Retrieved from: <http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx>

¹⁸ Organizations subject to PIPA must notify individuals when their personal information will be stored outside of Canada. The FOIP Act does not have this requirement.



importance of the service, the quantity and sensitivity of the information involved and the number and nature of changes to the service, among other things. Consider conducting annual reviews for cloud services that are important to school authority operations, or that involve potentially sensitive information.

It is common for cloud service providers to change their terms of service without warning or consultation. Changes often involve the service provider's privacy policies. This is much less likely to occur with negotiated contracts than with non-negotiable terms of service. When it happens, it is important to review the changes carefully to ensure that the school authority's privacy and security obligations can still be satisfied.



SECTION 3: PROTECTING PRIVACY WHEN SELECTING CLOUD SERVICES



SECTION 3: PROTECTING PRIVACY WHEN SELECTING CLOUD SERVICES

The following information complements the flowchart [Protecting Privacy When Selecting Cloud Services](#) on page 28. The flowchart provides a high-level summary of steps school authorities might use when analyzing needs, considering privacy and ultimately selecting cloud computing services for supporting learning and administration of education.

These practical steps take time and effort to undertake. Given this, the process recommendations are best suited for cloud services involving substantial privacy risks such as storage of highly sensitive personal information and/or services used throughout the school authority by a significant number of staff or students. Adapt these recommendations as needed for your context and situation.

See [Appendix G: Streamlining Cloud Service Selection/Approval Processes](#) for suggestions on how to streamline the selection process.

Note that this guidance is intended for school authorities subject to the Freedom of Information and Protection of Privacy Act (FOIP Act). Although much of it also applies to private school authorities subject to the Personal Information Protection Act (PIPA), they should consult their legal counsel and/or privacy officers before acting.

OVERVIEW OF PROCESS

The process of protecting privacy when selecting cloud services consists of three stages. The table below provides more information about each stage in the process.

Stage	Description
1 - Establishing priorities for the service	This stage involves determining the school authority's desired results, identifying if personal information is involved, and conducting a preliminary cost-benefit-risk analysis of key options for cloud services.
2 - Defining requirements and evaluating options	This stage involves determining available options for achieving desired results, assessing privacy protection requirements, and assessing the suitability of cloud service options.
3 - Selecting and contracting with a service provider	This stage involves selecting the preferred service provider, determining the contract and assessing residual risks to confirm the decision.



Consider documenting decisions and due diligence in a suitable manner while choosing a service provider. This may provide important evidence for your school authority if something goes wrong down the road.

Key privacy questions to consider when selecting a cloud service:

- **What is the nature and sensitivity of the personal information that will be stored in the cloud service?¹⁹**
- **What personal information is collected during use of the service?**
- **Who controls use of the personal information and what can the provider do with the data?**
- **Where is the personal information stored/accessed?**
- **Is personal information adequately protected and will privacy compliance requirements be met?**

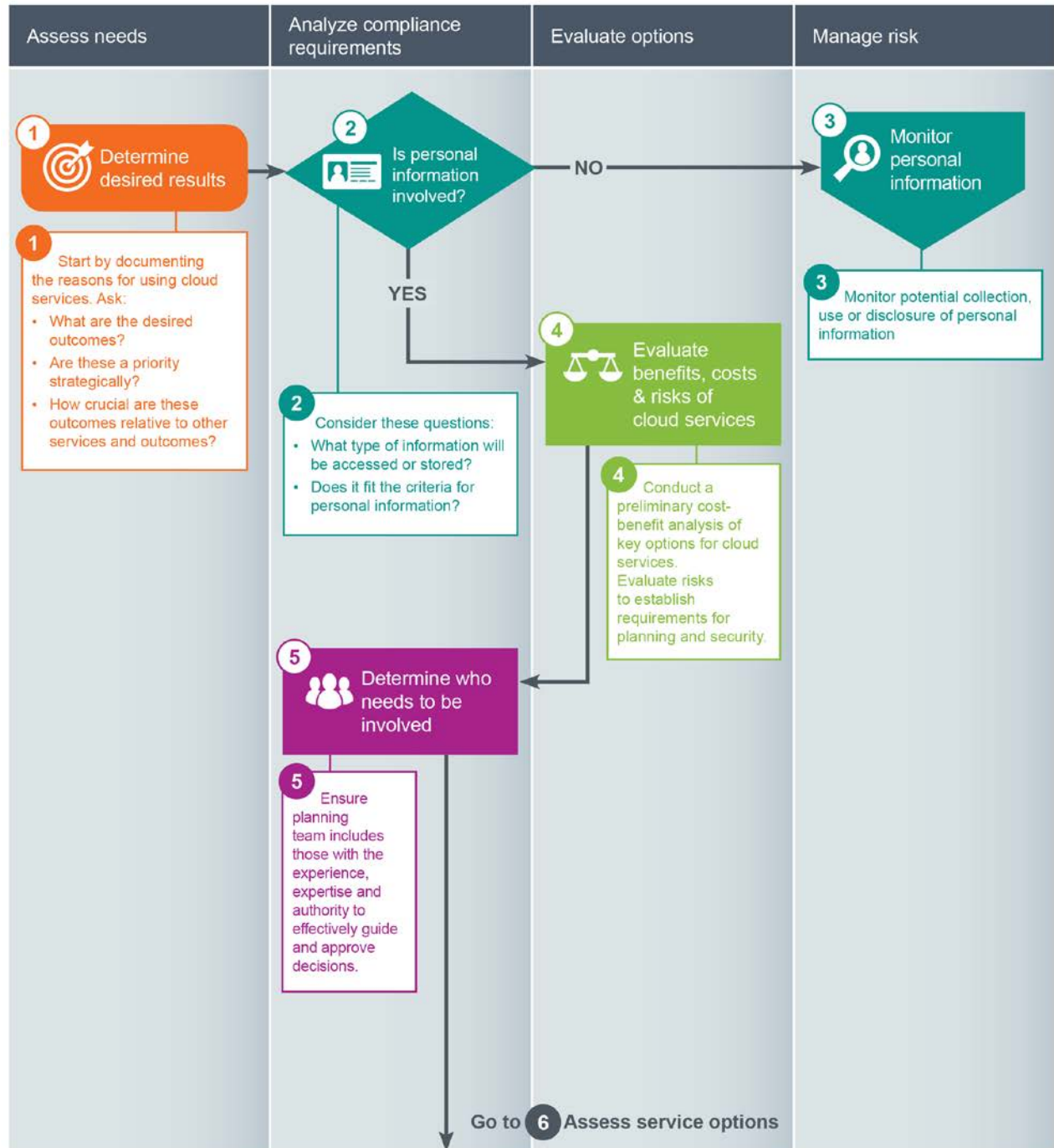
¹⁹ Moore, B. (2014). *Making Sense of Student Data Privacy*. Retrieved from the Intel website:
<http://www.intel.com/content/dam/www/public/us/en/documents/reports/analyst-report-student-data-privacy.pdf>



PROTECTING PRIVACY WHEN SELECTING CLOUD SERVICES FLOWCHART

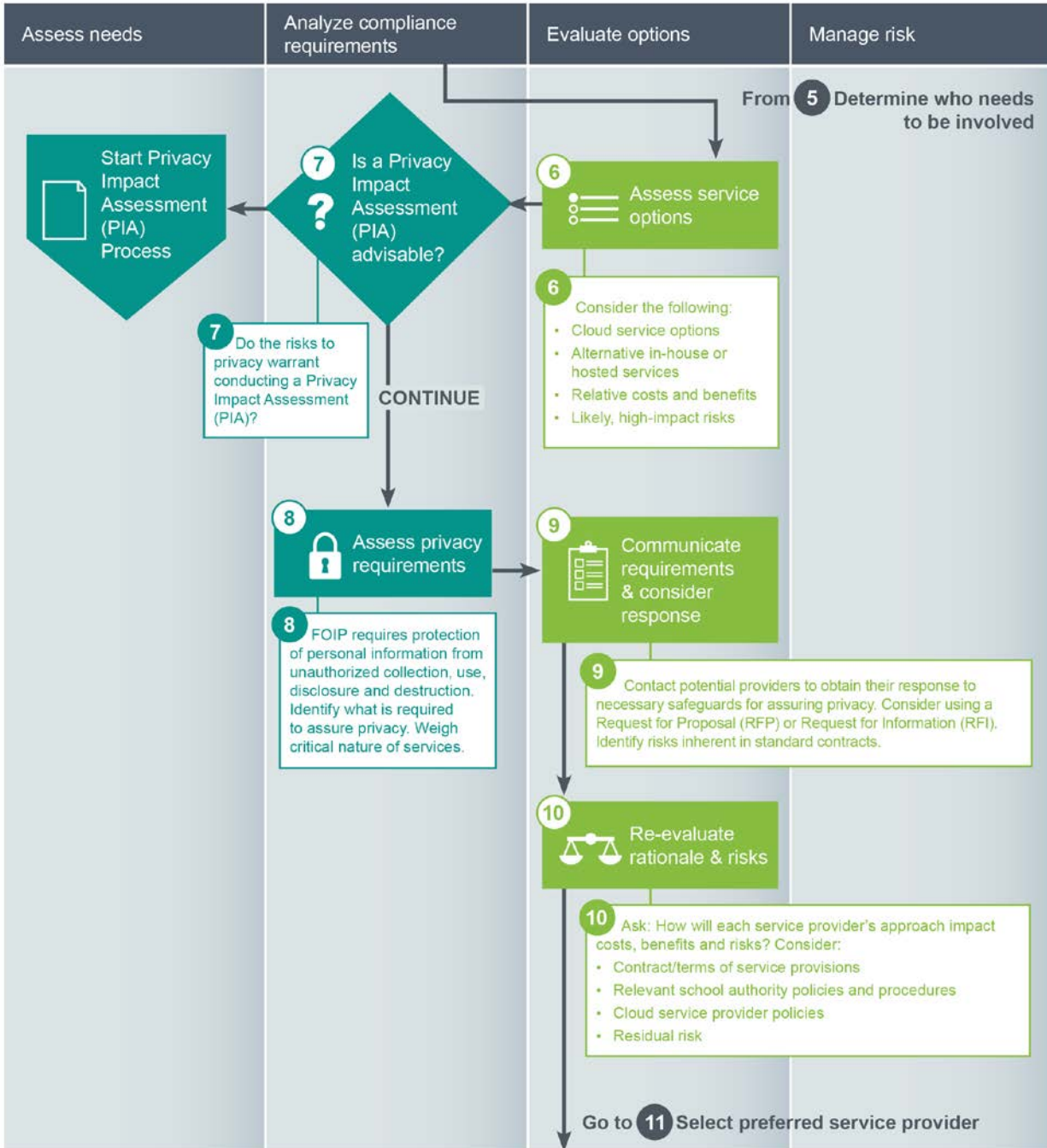
STEP 1: Establishing priorities for the service

Suggested Activity Leads: ■ Superintendent/Principal ■ FOIP Coordinator ■ ET Lead/IT Lead ■ Depends on project



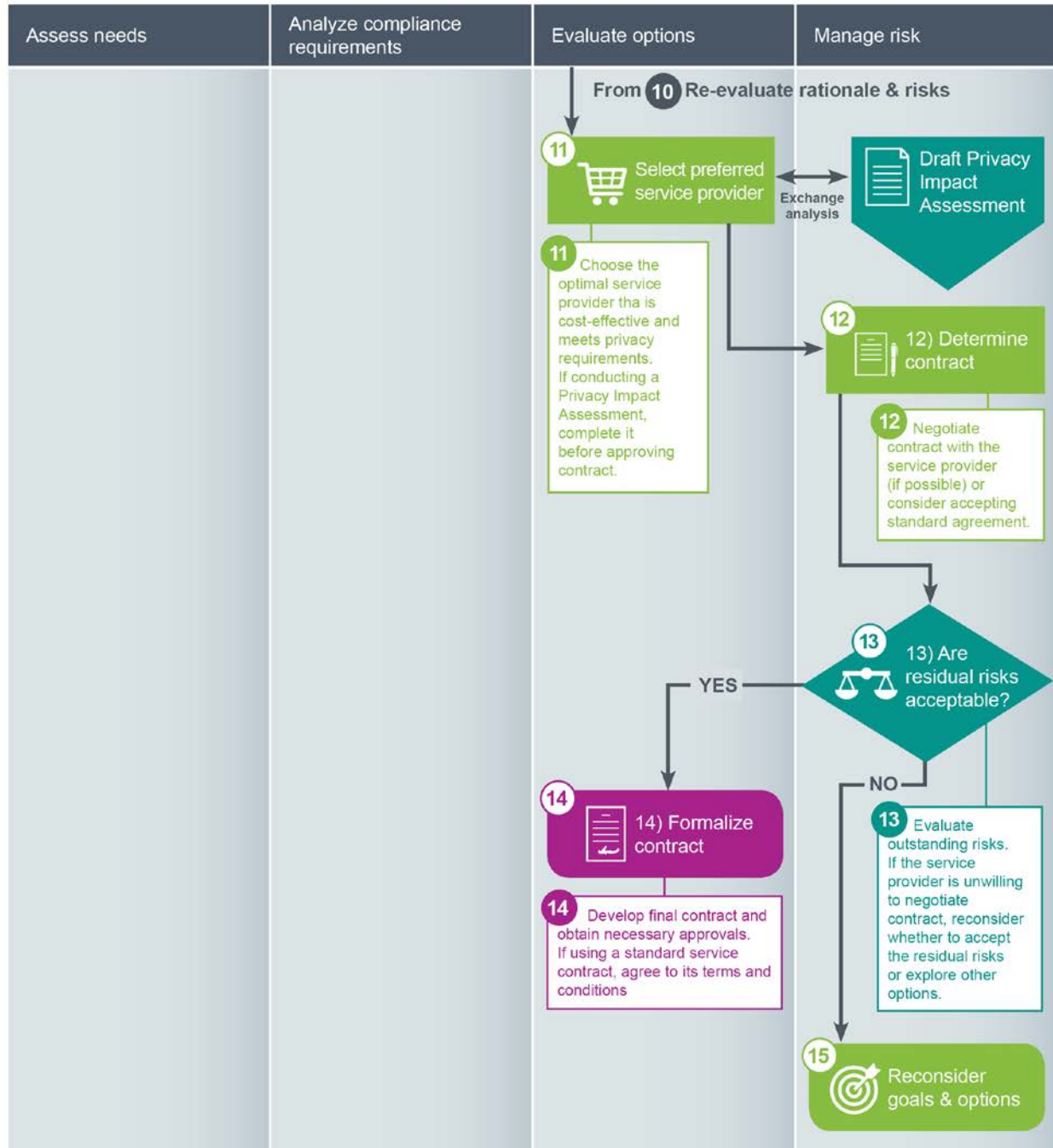
STEP 2: Defining requirements and evaluating options

Suggested Activity Leads: ■ Superintendent/Principal ■ FOIP Coordinator ■ ET Lead/IT Lead ■ Depends on project



STEP 3: Selecting and contracting with a service provider

Suggested Activity Leads: ■ Superintendent/Principal ■ FOIP Coordinator ■ ET Lead/IT Lead ■ Depends on project



The following information provides additional guidance for each step in the preceding flowchart.



STEP 1: DETERMINE DESIRED RESULTS

Start by identifying the desired outcomes as a preliminary step in considering whether to use cloud services.

Key questions for this step include:

- **What are the desired outcomes?**
- **In what ways are these outcomes aligned with the school authority's strategic priorities?**
- **How important are these outcomes relative to other desired services and related outcomes?**



STEP 2: IS PERSONAL INFORMATION INVOLVED?

After determining the desired results of using a cloud service, the next step is to assess the type of information that would be stored or accessed in the service. If personal information is involved, it is important to determine what legislation may govern the collection, use or disclosure of the information.

In order to make this decision, consider the following:

- The type of the information (i.e., demographic, financial, medical, school events, minutes of meetings, employment information, etc.) that would be collected, used, disclosed or stored in the cloud service. This could include personal information from a variety of sources, including employees, students, parents/guardians and others.
- Whether [personal information is involved as defined in section 1\(n\)](#) of the FOIP Act.
- Other applicable legislation that may govern the collection, use or disclosure of the information such as PIPA. If personal information is involved, the FOIP Act applies for public, separate and charter school authorities and PIPA applies for private schools.



If personal information is not involved, still consider doing a threat and risk assessment as other types of sensitive information about the operation of the school may be involved. It is important to address other measures such as security, information management and return of records upon termination of the service.

Note: Contact your FOIP office, FOIP co-ordinator or privacy officer if you have any questions about identifying personal information or about applicable legislation.



STEP 3: MONITOR PERSONAL INFORMATION

Initially, a school authority may not intend to use cloud services to collect, use, disclose or store personal information. However, a school authority's use of cloud services frequently evolves. Furthermore, personal information can be inadvertently contained in a wide range of documents and materials that the school authority may choose to store in a cloud solution. To manage this risk, school authorities might do the following:

- Periodically reassess if personal information is being collected or stored in a cloud initiative that did not initially include personal information.



- Recognize that any cloud service that enables storing unstructured²⁰ data increases the risk that personal information will be collected and stored in the cloud inadvertently.
- Reduce the impact of other potential risks by considering security and information management issues (i.e., defining a process for returning records when the service is terminated).



STEP 4: EVALUATE BENEFITS, COSTS AND RISKS OF CLOUD SERVICES

Conduct a preliminary analysis of the benefits, costs and risks of using a cloud service compared with other options. If it makes sense to proceed, school authorities can benefit from evaluating the risks inherent in various service options.

When determining the rigour of planning, risk management and consultation needed to adequately address school authority risks, consider the following:

Considerations	Potential Impact
Sensitivity of the information	<p>Section 38 of the FOIP Act requires protection of all personally identifiable information in the custody or control of a school authority subject to FOIP.</p> <p>The FOIP Act makes no distinction, but in practice some types of information are more sensitive than others (i.e., Social Insurance Number numbers versus email addresses) and may require additional protection, such as stronger security measures.</p> <p><i>See Step 10 for a discussion of sensitivity of personal information as it relates to residual risk</i></p>
Legislation governing the information	<p>If personal information is involved, then the FOIP Act applies.</p> <p>It is highly recommended that each school authority's FOIP co-ordinator and legal counsel is involved in all decisions related to privacy and FOIP compliance.</p>
Service criticality	<p>Mission critical services such as Student Information Systems are essential to the operation of a school authority. Any problems or disruptions with these and other core services likely will significantly disrupt the organization's operation.</p>
Location	<p>Information stored or in transit outside of Canada may be subject to foreign laws.</p> <p>Foreign cloud service providers may not comply with Canadian privacy laws. This may increase the risk to school authorities that are accountable for the actions of their foreign service providers under the FOIP Act.</p>

²⁰ Unstructured data include word processing documents, images, and other files that are not stored in formal databases.



Scope and scale	Services used by a large number of people within a school authority often require more research, consultation and risk management than single-use instances of software.
Public interest & perceptions	High profile projects may involve a higher level of reputational privacy risk. <i>Although only actual privacy breaches violate the privacy provisions of the FOIP Act, even the perception that privacy may not be adequately protected can seriously damage the reputation of a public body.</i> ²¹
Existing policies & procedures	School authorities may not have entered into similar agreements before and may not have policies or guidelines in place. In these cases, more time and consultation will likely be required when selecting new cloud services.



STEP 5: DETERMINE WHO NEEDS TO BE INVOLVED

When selecting a cloud service, it is critical to involve the right stakeholders to ensure effective management of value, cost and risk as well as assurance of privacy.

[Step 4.1: Define Roles and Responsibilities](#) in Section 2 of this document includes more information about which stakeholders may need to be involved.

Existing school authority policies, procedures or guidelines regarding selection and approval of cloud services may be of use when determining who should be involved in selecting a particular cloud service.

If in doubt about who should be involved from a privacy perspective, contact your FOIP co-ordinator or privacy officer.



STEP 6: ASSESS SERVICE OPTIONS

Research and identify potential service providers. Possible questions include:

- Which service providers are capable of meeting school authority needs?
- Are there viable in-house or hosted options?
- How closely will each option meet school authority needs?
- In general, what are the relative costs and benefits of each service?
- What are the high-likelihood and high-impact risks for the services?

Through the above questions, the school authority can identify its top choices.



STEP 7: IS A PRIVACY IMPACT ASSESSMENT (PIA) ADVISABLE?

Before continuing, consider whether or not to conduct a privacy scan, or a PIA, if personal information is involved. A PIA or privacy scan provides an opportunity and mechanism to show evidence of due diligence in identifying potential privacy risks and reasonable measures to mitigate the impacts.²²

²¹ Service Alberta. (2009). Privacy Compliance. *FOIP Guidelines and Practices: 2009 Edition*. Pg. 328. Retrieved from Service Alberta's website: <http://www.servicealberta.ca/foip/documents/chapter9.pdf>

²² A PIA is usually conducted once a service provider has been selected but you can begin gathering information for the PIA earlier.



Completing a PIA is not mandatory under the FOIP Act, but is strongly recommended by the Office of the Information and Privacy Commissioner (OIPC) and Alberta Education for any significant cloud computing initiative that involves identifiable personal information. Working through the PIA can contribute to the quality of the decision-making process; it is not merely a formality to complete after making a decision.

Completing a PIA does not exempt the school authority from possible sanctions due to privacy breaches or non-compliance with the FOIP Act; however, if a privacy breach occurs, previous OIPC acceptance of a PIA may be considered a mitigating factor. PIAs are not required to be submitted to the OIPC but can be done to document the due diligence process associated with a cloud computing decision.

If proceeding with a PIA, complete it before signing or accepting the contract if possible. Consult with your FOIP co-ordinator for more information.

Refer to [Appendix F: Risk Management Considerations and Approaches](#) for more information.



STEP 8: ASSESS PRIVACY REQUIREMENTS

The FOIP Act requires that school authorities protect personal information in their care and assure that it is protected from unauthorized collection, use, disclosure and destruction. School authorities cannot contract out of their obligations under the FOIP Act.

Contract provisions are key to mitigating the risks to privacy and achieving compliance with the FOIP Act. Suggested contractual provisions include retaining ownership of personal information, ensuring appropriate collection, use, disclosure, and destruction of personal information, and ensuring adequate breach identification and response procedures. Consider involving your FOIP co-ordinator and legal counsel in the development or review of contracts and service agreements.

Consider how to evaluate a service provider's ability to meet school authority privacy requirements. Using recommendations available in this document and other resources and counsel as appropriate, prepare a set of questions and requirements for potential cloud providers. Questions should cover all aspects of risk discussed. Requirements might include a set of contractual provisions.

Possible criteria for evaluating service providers include:

- Service provider's reputation.
This is an important consideration. Seek quality service providers with strong reputations, which can be expected to be in business for the long term.
- Service provider's policy on secondary uses of personal information.
School authorities are advised to avoid cloud providers who may attempt to use school authority data for unapproved secondary purposes.
- Location of the data centre(s) of the cloud service provider.
This is a key consideration due to the differences in privacy laws between Canada and other countries.
- Service provider's willingness to use non-standard service agreements.
This may be necessary to incorporate minimally acceptable privacy provisions.
- Service provider compliance with the laws of Canada or Alberta.
- Service provider support for FOIP access request processes.
- Service provider support for incident or privacy breach management processes.



- Service provider business structure.
Long-standing publicly traded companies are often considered less risky than privately held companies or those with little history, as it is easier to evaluate their reputation and financial viability.



STEP 9: COMMUNICATE REQUIREMENTS AND CONSIDER RESPONSE

Contact potential providers to obtain their feedback about the school authority's questions and the proposed contractual requirements. For large-scale cloud deployments, consider following a formal Request for Proposal (RFP) or Request for Quotation (RFQ) process.

For smaller deployments or for providers who do not respond to RFP or RFQ solicitations, it may be sufficient to contact providers more informally or review their terms of service, privacy and security policies.

Note: Many cloud service provider business models depend on using standard contracts and uniform services to benefit from economies of scale. Service providers may not be willing to negotiate terms of contractual agreements, and these providers are not suitable for initiatives involving personal information unless it has been determined that their standard privacy and security measures are sufficient to support the school authority's FOIP obligations. At a minimum, the service provider needs to have measures to give effect to FOIP rules if collecting, using or disclosing personal information on behalf of a public body, even if those measures do not include explicit references to the FOIP Act. Other provisions, such as specific security requirements may be desirable. It is reasonable to ask for specific provisions when making decisions about core systems critical to the school authority.

If the service provider's standard privacy and security measures do not meet FOIP requirements and the provider will not consider making any changes, your school authority should reconsider using the service.



STEP 10: RE-EVALUATE RATIONALE AND RISKS

As part of the procurement process, consider the proposals and other responses (if any) to the authority's requirements. How will each service provider's approach impact the costs, benefits and risks?

Additional considerations for managing risk:

- **Review contractual provisions**, considering both what is and what is not specified in the contract.
If personal information is involved, the contract should incorporate references to measures to protect privacy to FOIP standards. See [Step 4.6: Manage cloud service providers](#) in Section 2 for some suggested contractual provisions.
- **Review the service provider's security and privacy policies.**
These should be equivalent to school authority security and privacy policies. Note that encryption, for information both in transit and at rest, can be an important risk mitigation



strategy for ensuring the privacy and security of personal information, especially if the school authority retains control of encryption keys.

- **Review service provider’s security practices.**

A full security threat/risk assessment will rarely be feasible for a cloud service provider as they will not want to share such confidential information. However, questions can be asked to determine if the service provider has sound procedures for access control, employee security, encryption, intrusion detection, anti-malware issues, physical security and other aspects of data centre and network security.

- **Review information management considerations.**

In what cases could the service provider deny access to school authority records? How easily can the school authority remove data from the service provider? Does the service provider archive data for the required retention lifecycle? Are there mechanisms to ensure appropriate destruction of data as needed?

- **Complete the Privacy Impact Assessment (if applicable).**

A PIA is recommended to support any implementation decision concerning a large-scale cloud service that involves personal information.

- **Consider residual risks.**

It is not possible or feasible to eliminate all risk. Reducing the level of risk often involves time or resources. It is important to consider the value and cost of risk mitigation measures to determine which risks to mitigate. The risk that remains is referred to as residual risk and is a factor in determining whether to proceed. School authorities may want to adjust their level of acceptable privacy risk based on the sensitivity of the personal information involved, the location of the service provider, the provider’s reputation, etc.

See [Appendix H: Assessing Residual Risk](#) for more information.

Consider reviewing school authority policies and procedures to determine if they are up-to-date and sufficient to address the selection and implementation of the cloud computing service.

If you choose to accept the residual risk, consider documenting the decision, including your assessment of the nature of the residual risk, the likelihood and severity, and your decision to proceed. This can be useful in the event of a privacy issue or breach.



STEP 11: SELECT PREFERRED SERVICE PROVIDER

Choose the service provider that best meets school authority needs in consideration of the benefits, costs, and risks. Consider in-house or hosted options if the residual risks of using cloud services are not acceptable.

Typically, legal counsel is consulted after key decision makers have selected the service provider, if not earlier.

Note: If conducting a PIA, engage FOIP staff to commence the PIA process and review the contract before signing, if possible.²³

²³ PIAs are normally started after selecting the desired service provider. It is possible to conduct broader PIAs on more than one service provider to identify the best one from a privacy perspective, but such PIAs can be complex and time-consuming.



STEP 12: DETERMINE CONTRACT

Negotiate the contract with the service provider (if possible) or consider accepting the standard agreement or terms of service.



STEP 13: ARE RESIDUAL RISKS ACCEPTABLE?

If the service provider is unwilling to negotiate the terms of a standard contract, reconsider whether to accept the residual risks or explore other options.

See [Step 10](#) and [Appendix H: Assessing Residual Risk](#) for more information on residual risk.



STEP 14: IF RESIDUAL RISKS ARE ACCEPTABLE, FORMALIZE CONTRACT

If the residual risks are acceptable and you are accepting a standard agreement, this step may just involve accepting the agreement and entering information to set up the service. Other cases could be more complex. There may be specific requirements to integrate the cloud service with existing school authority services and data, or to move the school authority data to the cloud.

Once the selection process is complete, other steps will need to be completed, such as training staff. While privacy legislation does not require that stakeholders be informed when storing personal information in the cloud, it is a good practice to inform them. Consider explaining the measures taken to ensure that privacy is protected and appropriate responses will take place in the event of a breach.



STEP 15: IF RESIDUAL RISKS ARE NOT ACCEPTABLE, RECONSIDER GOALS & OPTIONS

If residual risks are not acceptable, reconsider your goals and options. Perhaps cloud service providers will change their services or provide better terms of service in the future. In-house or hosted services may meet your needs better.



APPENDIX A: GLOSSARY

CLOUD COMPUTING

Cloud computing is a model for network or Internet access to shared resources, software and information. It is delivered as a service that computers or mobile devices can access on demand. Examples of cloud services include Google Apps for Education, YouTube, Skype and Blackboard. See the [Cloud Computing Tech Briefing](#)²⁴ for more information.

See [Appendix B: Cloud Computing Evolution and Benefits](#) for more information.

CONFIDENTIALITY

Assurance that personal information sharing is limited to a specific designated group.

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (FOIP ACT)

The [Freedom of Information and Protection of Privacy Act](#)²⁵ is Alberta's public sector access to information and protection of privacy law. It applies to public bodies to ensure that they are open and accountable to the public by providing a right of access to records; and to protect the privacy of individuals by controlling the manner in which public bodies collect, use and disclose personal information. Alberta public bodies include public and separate school boards, charter schools and regional authorities, as defined in the [School Act](#). A [high-level overview of the FOIP Act](#) is available.

INFORMATION PRIVACY

Individuals'²⁶ right to control the collection, use and sharing of their [personal information](#) with others.

INFORMATION SECURITY

Information security refers to “the processes and methodologies which are designed and implemented to protect print, electronic or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification or disruption...with the goal of protecting the confidentiality, integrity and availability of information.”²⁷

Section 38 of the FOIP Act requires “reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction of information.” Information security includes appropriate administrative measures (security policy, procedures, training, etc.), technical

²⁴ Alberta Education. (2013, May 1). *Cloud Computing Tech Briefing*. Retrieved from: <https://education.alberta.ca/media/3114992/cloud-computing-tech-briefing.pdf>

²⁵ Service Alberta. *Freedom of Information and Protection of Privacy Act*. Retrieved from Service Alberta's website: <http://www.servicealberta.ca/foip/>

²⁶ Or legal representatives of individuals, such as guardians.

²⁷ SANS Institute. *Information Security Resources*. Retrieved from the SANS Institute's website: <http://www.sans.org/information-security/>



measures (access controls, anti-malware, intrusion detection, etc.) and physical measures (locked doors and cabinets, alarm systems, etc.).

PERSONAL INFORMATION

Section 1(n) of the FOIP Act defines personal information as recorded information about an identifiable individual, including, but not limited to:²⁸

- 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, other biometric information, blood type, genetic information 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; and
- the individual's personal views or opinions, except if they are about someone else.

Note that these categories are illustrative, not exhaustive. Other information about an identifiable individual is also considered personal information. Also note that the definition does not include information about corporate persons.

PERSONAL INFORMATION PROTECTION ACT (PIPA)

The [Personal Information Protection Act](#)²⁹ is Alberta's private sector privacy law. It applies to provincial private sector organizations, businesses and, in some instances, to non-profit organizations for the protection of personal information. A [high-level overview of PIPA is available](#).

PRIVACY

Privacy is not defined in legislation. One common definition is "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment or accountability, and the attempt to control the time and manner of disclosures of personal information about ourselves."³⁰ Privacy is a human right and a fundamental freedom that is the cornerstone of other freedoms in our society. Privacy involves a number of aspects including physical, communication, behavioural and information privacy.

²⁸ Section 1(n) of the [Freedom of Information and Protection of Privacy Act](#) (FOIP Act)

²⁹ Service Alberta. *About the Personal Information Protection Act*. Retrieved from Service Alberta's website: <http://www.servicealberta.ca/pipa-overview.cfm>

³⁰ Smith, R. (2000, June). Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet. Pg.34.



PRIVACY BREACH

A privacy breach occurs when there is unauthorized collection, use or access to personal information.³¹

PRIVACY IMPACT ASSESSMENT

PIAs are used to identify the potential privacy risks of new or redesigned programs or services offered by an organization. They also help eliminate or reduce those risks to an acceptable level.³²

RECORD

The FOIP Act defines record as,

“a record of information in any form, including notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers, and any other information that is written, photographed, recorded or stored in any manner but does not include software or any mechanism that produces records.”³³

Any recorded information, including handwritten notes and electronic correspondence or messages, which is in the custody or control of a public body, is a record for the purposes of the FOIP Act.

SCHOOL ACT

The [School Act](#) describes the relationship of the Minister to students, parents and school jurisdictions and provides for the system of administration and financing of education in Alberta, and generally deals with the ultimate authority of the Minister with respect to all constituents in the educational system.³⁴

³¹ Office of the Information and Privacy Commissioner (OIPC). (2015, May). *Key Steps in Responding to Privacy Breaches*. Retrieved from the Alberta Office of the Information and Privacy Commissioner website:

https://www.oipc.ab.ca/media/652724/breach_key_steps_responding_to_breaches_jul2012.pdf

³² Office of the Privacy Commissioner of Canada. (2011, December 23). *Privacy Impact Assessments*. Retrieved from the Office of the Privacy Commissioner of Canada website: https://www.priv.gc.ca/resource/fs-fi/02_05_d_33_e.asp

³³ Section 1(q) of the [Freedom of Information and Protection of Privacy Act](#) (FOIP Act)

³⁴ Alberta Education. *School Act and Regulations*. Retrieved from the Alberta Education website: <https://education.alberta.ca/department/policy/legislation/regulations.aspx>



APPENDIX B: CLOUD COMPUTING EVOLUTION AND BENEFITS

EVOLUTION OF CLOUD COMPUTING

Before cloud computing became available, school authorities managed technology such as servers, storage and software licenses on site or through outsourcing to hosting providers.

Cloud computing was envisioned as a way for organizations and individuals to access computing resources on demand like a utility service such as power. As high-speed bandwidth became available, software companies started delivering applications and infrastructure services through the Internet and cloud services gained in popularity.

BENEFITS OF CLOUD COMPUTING

Cloud services offer many compelling benefits over traditional technology management and outsourcing practices.

Benefit Type	Description
Learning	<ul style="list-style-type: none">• Personalized learning. Cloud computing provides opportunities for greater student choice in learning. Using an Internet-connected device, students can access a wide variety of resources and software tools that suit their learning styles and interests.
Administrative	<ul style="list-style-type: none">• Minimal set-up and maintenance requirements. Many cloud services can be set up in a matter of minutes with no need to apply patches or upgrades.• Reduced capital investment costs. Cloud-based services provide access to full featured applications or infrastructure services with minimal up-front investment in hardware servers and storage. Cloud services can be accessed from any device or computer that has network connectivity; there is no need to purchase and maintain hardware or pay for staffing costs to apply patches to applications. This can provide an innovative and flexible approach to managing technology investments.



APPENDIX C: HOW DOES USE OF CLOUD SERVICES IMPACT PRIVACY?
















School authorities collect and use large quantities of student and employee information for learning, instruction and administration of education. They have always been accountable for protecting the privacy of the personal information in their care and have done so through measures such as locking file cabinets, securing information on their hard drives and developing policies.

As the use of cloud services has grown, significant amounts of personal information have moved from the direct control of school authorities to the control of cloud service providers. This has introduced new privacy risks related to the loss of direct control over data management and other privacy-relevant aspects of cloud computing services.



Cloud computing differs from traditional on-premise technologies and outsourcing in a number of fundamental ways that significantly affects the ability to protect privacy.

Comparison of Privacy Considerations for On-premise, Hosted and Cloud-based Services

Category	On-premise	Hosted	Cloud	Cloud Privacy Implications
Where is personal information physically located?	 Within your jurisdiction	 Known physical location outside of your jurisdiction	 In one or more data centres anywhere in the world	Cloud service providers outside of Canada are not required to comply with Canadian privacy legislation unless that is specified in the agreement.
How much control does school authority have:				
Over contract terms?	 Full control – deal directly with vendors	 Negotiate and mutually agree on contract terms	 <ul style="list-style-type: none"> Usually must accept standard terms of service. Terms are heavily weighted in provider's favor. Provider can change terms at any time. 	Contract terms may impact ability to comply with privacy legislation and to effectively manage privacy risks. Standard terms may not ensure compliance or provide remedies if there are breaches.
Over personal information?	 Full control: personal information is in the school's custody	 As per negotiated terms of agreement	 Usually minimal control and ability to negotiate to: <ul style="list-style-type: none"> retain ownership of personal information ensure appropriate collection, use and sharing of personal information. 	
Who is responsible for managing/storing personal info?	 School authority	 Third party provider	 Cloud service provider	The cloud service provider has significantly more access to and control over personal information.
Who is accountable for ensuring appropriate collection, use and sharing of personal information?	 School authority	 School authority	 School authority	Your school authority is accountable for actions of cloud service providers even though it may have little ability to negotiate appropriate contract terms.

Traditional hosted or outsourcing agreements offer limited lessons for the management of cloud services, as cloud service contracts are usually not subject to negotiation, especially for free or low cost cloud services. Adopting a cloud computing service is often a take-it-or-leave-it proposition. Standard contracts or terms of service often favour the rights of the provider and may not ensure compliance with privacy legislation or provide remedies if there are breaches. This is an important consideration, especially when the provider has not considered compliance with Canadian privacy law, since the FOIP Act does not allow a public body to contract out of its FOIP obligations.

Depending on the nature of the cloud service and related contractual terms, it may be more difficult to ensure compliance with the FOIP Act and related security requirements than for a similar service that is locally hosted and managed. Such issues can often be managed, especially if contractual terms can be negotiated, but they require careful attention to privacy and security compliance obligations and related contractual terms.

Since contract terms are often not negotiable, procuring cloud services then involves comparing available options and selecting the best choice (or not storing personal information in the cloud if the personal information is sensitive and the risk is too great).

The impact of cloud services on privacy is greatly reduced if there is little or no personal information sent to the cloud. Where possible, it is always preferable to minimize the amount of identifiable personal information that is sent to the cloud.

Even cloud services that require personal information can sometimes be used without involving *identifiable* personal information, by de-identifying the information prior to storing it in the cloud. Although such “anonymization” approaches can be effective, they should be taken with care, as it may be possible to re-identify individuals more easily than it appears.³⁵

³⁵ See the examples provided in the following paper, which argues in favour of anonymization approaches but cites examples where data can be re-identified.

Cavoukian, A. Emam, K. (2011, June). *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy*. Pg. 1-2. Retrieved from the Ontario Information and Privacy Commissioner website: <https://www.ipc.on.ca/images/Resources/anonymization.pdf>

APPENDIX D: PRIVACY LEGISLATION CONSIDERATIONS

Privacy legislation is intended to ensure that organizations do not unjustifiably reduce individuals' control over their own personal information. Privacy legislation gives individuals the right, with limited and specific exceptions, to control the collection, use and disclosure of their personal information. Although privacy legislation predates modern information technology, it is technology that drives most of today's privacy issues. Cloud computing is no exception.

WHAT LEGISLATION APPLIES AND TO WHOM?

Public bodies in Alberta are subject to the *Freedom of Information and Protection of Privacy Act* (FOIP Act). This includes public and separate school boards, charter schools and regional authorities, as defined in the [School Act](#). The FOIP Act is available from the [Alberta Queen's Printer](#). Consult your *Freedom of Information and Protection of Privacy* (FOIP) co-ordinator and legal counsel for more information.



Private schools are not covered by the FOIP Act, but are covered by similar legislation for the private sector, the [Personal Information Protection Act \(PIPA\)](#). While PIPA is based on principles similar to those on which the FOIP Act is based, the details of the two Acts differ. Therefore, private schools should review their PIPA obligations before applying the guidance in this document.

It is important to take note of any variances in FOIP rules that may arise from other legislation to which the school authority is subject, notably the *School Act* as well as its regulations.

Canadian cloud service providers are directly subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and, in some cases, equivalent provincial legislation such as the *Personal Information Protection Act* (PIPA) in Alberta. This means that they are required to abide by a set of privacy principles that are similar, albeit not identical, to those that form the basis of the FOIP Act and most other Canadian privacy law. They are also bound by the FOIP Act as employees of the school authority for the services that they provide to the school authority.

United States privacy law is very different from Canadian privacy law. The United States has no national privacy law, nor does any US state have general privacy legislation comparable to PIPEDA or the laws of Canadian provinces. Privacy law in the United States is sector-specific and issue-oriented. Privacy law is largely absent in the United States IT industry except for certain legislation intended to address specific issues, such as breach notification and online privacy for children, and the Federal Trade Commission's enforcement of truth-in-advertising principles.

United States cloud computing service providers do not normally attempt to comply with non-US law. Many of their service agreements specify that compliance with non-US law is the sole responsibility of the client. Therefore, it is important to ask what procedural and substantive laws govern their services and what the resulting implications might be for Canadian customers.

If using a service provider puts the school authority in a potential position of legal noncompliance, the school authority must decide either not to use the service, or to use it despite the risk of noncompliance. This decision will depend on the school authority's assessment of the nature, likelihood and severity of



the risk and the consequences of noncompliance. However, school authorities should never accept a highly probable risk of serious noncompliance.

The school authority's FOIP co-ordinator and legal counsel should be involved in all decisions related to freedom of information and privacy issues arising from matters of FOIP compliance. The FOIP co-ordinator should be the primary resource for the management of FOIP issues, with legal counsel providing a supporting role as necessary.

IS STORING OR ACCESSING PERSONAL INFORMATION OUTSIDE OF CANADA ALLOWED?

Yes. However, your school authority is still accountable for ensuring compliance with privacy legislation and that accountability cannot be delegated to a cloud service provider. Requirements include ensuring adequate protection of personal information and confirming that records can be accessed and corrected within a reasonable time frame if requested by a parent or student.

IS COMPLYING WITH THE FOIP ACT ENOUGH?

Complying with the FOIP Act is a legal requirement. Technology changes more rapidly than legislation. Consider adopting a comprehensive approach to protecting student privacy (as discussed in [Section 2: Considerations for Assessing Readiness for Cloud](#)) to more efficiently and effectively protect personal information in the cloud.³⁶

³⁶ Privacy Technical Assistance Centre. *Protecting Student Privacy While Using Online Educational Services*. Pg. 5. Retrieved from U.S. Department of Education's website: <http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services>



APPENDIX E: KEY CHALLENGES OF MANAGING CLOUD PRIVACY RISKS

Cloud services pose a number of challenges to ensuring effective governance, risk management and compliance with privacy legislation including:

- **Challenges listed in [Section 1: Key Concepts](#).**
- **Challenges managing third party plugins or controls.** Cloud service providers often allow other vendors to create plugins or controls that work with their cloud service platform. These third party plugins or controls usually have different terms of service than the cloud platform. School authorities may have conducted a Privacy Impact Assessment on the cloud service platform but need to remember that each third party plugin or control should be evaluated separately to determine if privacy risks can be adequately managed.
- **Overestimating the level of risk.** Overestimating the level of privacy risk may result in missed opportunities to leverage the benefits of cloud services for learning and administration. For example, cloud services that require no personal information, other than perhaps some business contact information for a teacher or administrator, pose much less privacy risk than those that require personal information about identifiable students.
- **Rapid evolution of privacy risks.** With the increasingly pervasive use of technology in everyday life, new technologies may change the nature of privacy risks or introduce additional risks.
- **Unclear roles and responsibilities.** A lack of clarity regarding who is accountable and responsible and lack of communication between key decision makers may detrimentally affect the quality of decisions made.
- **Varied understanding of cloud computing and privacy-related matters.** Lack of awareness and understanding regarding legislation and compliance requirements can result in acceptance of significant privacy risks without understanding the implications.
- **Favouring convenience over privacy.** If people do not understand why it is important to protect privacy, they may trade privacy for convenience. This can happen with organizations as well as individuals.



APPENDIX F: RISK MANAGEMENT CONSIDERATIONS AND APPROACHES

This appendix provides information about risk management considerations and approaches. It is important to be aware of privacy risks associated with a cloud service before committing to it. The assessment of such risks may range from cursory to extensive, depending on the nature, sensitivity and volume of personal information involved, the nature and terms of service of the cloud service, the likelihood and severity of a privacy breach, and other factors.

Consider conducting a level 1 risk assessment for all cloud services being evaluated for use at a school authority and a level 2 risk assessment or higher depending on the nature and sensitivity of the personal information and other factors. See the sections below for more details.

The following resources will assist in conducting privacy scans and privacy impact assessments:

- [Privacy Impact Assessment Requirements](#)³⁷ from the OIPC
- [Service Alberta PIA templates](#)

LEVEL 1 RISK ASSESSMENT

Review cloud service provider privacy and security measures, especially those specified in its terms of service, privacy policy and security policy.

Whenever a school authority is contemplating adopting a cloud service, it should carefully review the privacy and security measures to which the service provider is prepared to commit in its terms of service. This is especially important when the terms of service are non-negotiable, but is also important even if the contract may be subject to negotiation, since the standard privacy and security measures are the ones that are most likely firmly embedded within the service provider's operations.

Many cloud service providers will also provide documentation of privacy and security measures that are not explicitly referenced in the terms of service. These are also important to review, although measures that are not referenced in the terms of service may not be subject to contractual enforcement.

The location of data can be important in cloud service arrangements. Try to ascertain where data is housed, especially whether it is housed inside or outside Canada. Also, ascertain whether the service provider is subject to Canadian laws or those of another country, which can affect how easily contractual terms can be enforced.

This level of assessment should be conducted for every cloud service being considered by a school authority, before any contract is signed or terms of service accepted. It is also recommended for any cloud service that the school authority already uses if a risk assessment has not already been conducted for that service.

³⁷ Note that the requirements from the Office of the Information and Privacy Commissioner (OIPC) apply to PIAs conducted for compliance with the *Health Information Act*, but they can also be used for FOIP PIAs with minor adjustments.



LEVEL 2 RISK ASSESSMENT: CONDUCT A PRIVACY SCAN

This type of risk assessment is known by various terms, but it refers to a preliminary or summary analysis of privacy risks, which would normally be focused on compliance with legislation and school authority policy. Essentially, the privacy scan is intended to identify any aspect of the cloud service that would make it difficult for the school authority to comply with its own policy, or with relevant legislation.

The [PIA template provided by Service Alberta](#) is an example of a privacy assessment at this level. (An equivalent security assessment would involve questions to determine compliance with school authority security policies and practices, as well as security standards with which the school authority seeks to comply.) This level of assessment is important for any cloud service that will involve the personal information of identifiable students or school authority employees³⁸.

It is recommended that a privacy scan be conducted on any currently used cloud service if the service involves the collection, use or disclosure of personal information, if one has not already been done.

LEVEL 3 RISK ASSESSMENT: CONDUCT A COMPREHENSIVE PRIVACY IMPACT ASSESSMENT

A comprehensive Privacy Impact Assessment (PIA) involves an assessment of privacy risks and mitigation measures, in addition to the compliance assessment involved in a privacy scan. A comprehensive PIA will assess not only compliance with applicable legislation and policy, but also other considerations pertinent to the management of privacy risks, regardless of the extent to which existing legislation and policy may make reference to such risks.

The best available example of a comprehensive privacy impact assessment in Alberta is contained in the [Privacy Impact Assessment Requirements](#) provided by the Alberta Office of the Information and Privacy Commissioner (OIPC). While these requirements are mainly intended for use with the *Health Information Act*, they can also apply to privacy impact assessments prepared by FOIP public bodies, with only minor wording changes.

A comprehensive PIA may be appropriate for a cloud service currently in use if unmitigated privacy risks are suspected or known to exist, especially as the result of a privacy scan. A comprehensive PIA is also recommended if the cloud service would host or process very sensitive personal information (i.e., information related to the health or welfare of students, or human resources), or large volumes of personal information.

In addition to these three levels of risk assessments, the Law Society of British Columbia has prepared a list of cloud computing [due diligence considerations](#) for its members.³⁹ These considerations could be useful for school authority legal counsel and FOIP co-ordinators in assessing cloud computing services.

³⁸ In the case of employees, basic business contact information, such as that found on a business card or business-related online service registration, is usually of less concern than other kinds of personal information.

³⁹ Cloud Computing Working Group. Law Society of British Columbia. (2012, January). *Cloud computing due diligence guidelines*. Retrieved from www.lawsociety.bc.ca/docs/practice/resources/guidelines-cloud.pdf



APPENDIX G: STREAMLINING CLOUD SERVICE SELECTION/APPROVAL PROCESSES

Many online educational services and mobile applications currently employ Terms of Service (TOS) Agreements. These types of agreements are often referred to as *click-wrap* software agreements. For users to access the service or application, they are asked to click *I agree* to the terms of service. Once the terms of service are agreed upon, these will determine the information the service provider is allowed to collect from or about students and staff, what it can do with this information and how the information might be shared.

In many cases, the terms of service embedded in click-wrap agreements do not allow the user to comply with their privacy legislation obligations. School authorities reduce the risks associated with these services by understanding standard terms of service provisions and establishing policies that will guide users in determining whether to agree with any proposed terms of service.

The following are practices that school authorities might use to streamline the cloud service selection and approval process:

- Review terms of service and related privacy and security policies for select cloud providers and services. Determine evaluation criteria related to privacy, security and other factors. Then, establish a list of preferred cloud services and provide a mechanism for staff members to request evaluation of cloud services they would like to use.
- Designate employees in the school authority who are authorized to evaluate and accept provider agreements or terms of service. Ensure that these staff members have the necessary knowledge and skills to assess the privacy and security implications of cloud services and know when to involve leaders in making the decision.
- Consider developing guidelines for cloud services that are used sporadically by a small number of people with information that tends to be less sensitive, such as apps or cloud services that do not require personal information. Decisions about these systems may be delegated to educators and school leaders provided they have the guidance, skills and authority required to evaluate and mitigate any potential privacy risks.



APPENDIX H: ASSESSING RESIDUAL RISK

After you have done all you can to minimize privacy risks associated with a given cloud computing service, it will be necessary to determine what residual risk remains. That residual risk will be the determining factor in your decision whether or not to proceed. If you choose to accept the residual risk, there should be a documented decision to this effect, which states the nature of the residual risk, your assessment of its likelihood and severity, and your decision to proceed despite it.

The acceptance of residual risk is something that organizations do all the time. It is never possible to completely eliminate all risk; the best that can ever be done is to eliminate the risks that can be eliminated, mitigate as best as possible the ones that cannot be eliminated and decide whether the remaining risk is acceptable.

While there is no fixed standard for acceptable residual risk, it is worthwhile considering some factors that may mitigate or exacerbate residual risk, depending on the circumstances.

1. *Sensitivity of Personal Information*

The FOIP Act does not distinguish between types of personal information. Information is either personal or it is not. Consequently, FOIP rules apply to all personal information, regardless of its sensitivity. The FOIP Act lists types of information that are explicitly deemed to be personal, but its privacy provisions apply to all information related to an identifiable individual. This is the case with most other privacy legislation as well.

In practice, however, some kinds of personal information are more sensitive than others. This means that differential levels of information protection may be appropriate in some circumstances. This is true of both local and cloud computing services.

From an information protection perspective, the most sensitive personal information is that which can identify an individual. This is the type of information that can easily be misused for nefarious purposes, such as identity theft and fraud. There are two types of identifiers, unique and non-unique.

Unique identifiers are those that identify one and only one person. Some are also lifetime identifiers, which never change for the person in question. Examples include the social insurance number, personal health number, driver's license number, individual bank account number, credit card number and others. The Alberta Student Number falls in this category, although it is used widely in the education system and considered less confidential than most unique identifiers. Unique identifiers are normally considered highly confidential.

Other identifiers will identify an individual person, but are not truly unique. These *non-unique identifiers* include a person's name, birth date, address, e-mail address, telephone number and various other kinds of personal information that we typically use to identify a person. These identifiers may be duplicated among multiple people, but usually the number of people they identify is small enough that a single person can be identified in many circumstances. Non-unique identifiers are widely used in day-to-day life and are not considered to be as confidential as unique identifiers.

However, non-unique identifiers can become unique or almost unique when used in combination. For example, a combination of full name, birth date and current home address will uniquely identify the vast majority of people, even though multiple people may have any one of these identifiers.



Therefore, non-unique identifiers may require as much protection as unique identifiers, despite the fact that they are not unique and may circulate widely. This depends on which identifiers are involved, how many of them there are and whether they can be used in combination to uniquely identify an individual.

Personal identifiers in general require a high level of privacy and security protection. If personal identifiers, especially unique identifiers, are to be included in information held by a cloud computing provider, it is very important that the school authority is confident in the provider's privacy and security measures and adequate contractual controls are in place. On the other hand, if the information to be held by the provider does not include personal identifiers, or only includes a few non-unique identifiers that are not easily used in combination, the school authority may be able to accept a somewhat reduced level of information protection without substantially increasing privacy risk.

Identifiers aside, people tend to view certain kinds of personal information as more sensitive than others. Over the years, various surveys have suggested that some categories of personal information are often, albeit not always, considered by most adults to be the most sensitive.⁴⁰ It may be wise to provide a level of privacy and security for these categories of information that is equivalent to that provided for identifiers:

- financial information (credit cards, financial accounts, credit reports, etc.)
- health-related information
- personal correspondence
- employment details such as salary and benefits, but not employment responsibilities.

Finally, it is safe to say that many parents consider personal information about children to be more sensitive than information about adults, all other things being equal. This is so despite the widespread use of social media by children. Organizations dealing with children's personal information, such as school authorities, may need to adjust their privacy risk appetite accordingly.

2. *Provider Jurisdiction*

The jurisdiction of the provider can be a significant factor in the assessment of residual risk. This arises mostly from the nature of privacy law in the provider's jurisdiction.

The United States has no national privacy law and the US information technology industry is not governed by sector-specific privacy law. In other jurisdictions, though, privacy protection is more codified. In the European Union, for example, privacy law provides a consistently high level of protection, although in some respects the legislation is significantly different from Canadian privacy legislation.

It might be reasonable to accept a somewhat higher level of residual privacy risk in a relationship with a provider operating under more rigorous privacy law than one operating in a less stringent environment. Jurisdictional comparisons are difficult to make, though, and the jurisdiction of the provider may be more significant in theory than in practice. Nevertheless, it is a factor to consider if it appears that there may be significant residual privacy risk associated with a given provider relationship.

⁴⁰ See, for example, *OIPC Stakeholder Survey, 2003*. (2003, March). GPC Alberta. Retrieved from https://www.oipc.ab.ca/media/614659/survey_population_survey_2003.pdf.



3. *United States Federal Trade Commission*

The United States Federal Trade Commission (FTC) enforces fair advertising principles in the IT industry and other industries.⁴¹ It requires that service providers live up to the public statements they make concerning their services, especially where privacy and security measures are concerned. This means that statements made publicly or posted on company websites concerning privacy and security measures, even if they are not reflected in standard service agreements, may carry some weight in law. In turn, this means that providers, especially large ones, may be more careful to ensure that the statements they make about their services are accurate.

This has two general effects. The first is to make such statements less specific and sometimes more vague than they might otherwise be. The second is to instill somewhat more confidence in such statements than one might otherwise have.

This can be a significant, albeit not deciding, factor in the assessment of residual risk is associated with cloud computing services. While cloud computing vendors' standard service agreements may not meet the standard for privacy and security that a school authority might want, in some cases ancillary documentation available from the provider gets closer to a desirable level of privacy and security protection. Because of FTC enforcement of such ancillary statements, those statements can sometimes be accepted with more confidence than would otherwise be the case. This is especially true if the statements have been the subject of an FTC investigation or order.

Because FTC investigations are usually complaint-based, a given service agreement or related information may not have ever been the subject of an FTC investigation. School authorities will need to use their best judgment in assessing whether FTC enforcement is a significant factor in assessment of residual risk on a case-by-case basis.

4. *Reputational Factors*

The reputation of the provider can be important in assessing residual risk. If the provider has a reputation for stringent protection of personal information, for resisting third-party demands for that information, and for being responsive to questions for improved privacy measures, a higher level of residual privacy risk in the providers' standard service agreement may be acceptable. Although it is always important to negotiate the best possible contract, if you need to accept a less than ideal contract, it is best to do so with a provider that has a good reputation for privacy protection.

Information about provider reputation usually must be obtained or inferred from media reports and reviews about the provider. It is wise to review media reports and other resources for privacy-related issues associated with a potential provider when considering or reviewing engagement with them. This can usually be accomplished with some well-worded Internet searches, but may require greater effort if such searches are unsuccessful.

⁴¹ See *Enforcing Privacy Promises*. US Federal Trade Commission. Retrieved from <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises>



APPENDIX I: ADDITIONAL RESOURCES

The following resources provide additional information that you may find of use.

1. [Freedom of Information and Protection of Privacy Act \(FOIP Act\)](#) and Regulation
This is the Act to which most school authorities (except for private schools) in Alberta are subject.
2. [Personal Information Protection Act \(PIPA\)](#) and Regulation
This is the Act to which private schools in Alberta are subject.
3. [FOIP Guidelines and Practices](#)
This manual provides comprehensive guidance on FOIP administration, including compliance with its privacy provisions.
4. [Cloud Computing for Small- and Medium-Sized Enterprises: Privacy Responsibilities and Considerations](#)
This guidance document is published jointly by the federal, Alberta and British Columbia privacy commissioners. While it is intended mainly for commercial organizations, which in Alberta are subject to PIPA, most of its guidance is applicable to small and medium-sized FOIP public bodies as well.
5. [NIST Guidelines on Security and Privacy in Public Cloud Computing](#)
These are among the most comprehensive cloud computing guidelines available, but they are intended for a public sector audience in the United States. While the discussion of cloud computing risks and mitigation measures is generally applicable for any public sector organization in North America, legislative references and inferences do not apply in Canada.

