

October 4, 2024

VIA ELECTRONIC MAIL:

Dear \_\_\_\_\_ :

**Re: Request for Access to Records – Response**  
***Freedom of Information and Protection of Privacy Act (FOIPPA)***

I am writing further regarding your request for access to records relating to the following:

- 1. Final job description files for any employee who regularly performs a role or responsibility (1) in responding to a freedom of information request or (2) fulfilling the public body's records/information management needs, including if those job descriptions do not explicitly mention FOI requests or records/information management.***
- 2. Records confirming the appointment and responsibilities of subdivisional freedom of information (not privacy) or records management 'champions,' (i.e. an ambassador for records management or FOI within a particular unit, such as FOI Oversight Liaison Officers or Duty to Document Champions), if any. (If applicable roles exist, kindly include memorandums or directives, plans, and/or reports issued by those persons).***
- 3. Organizational charts that include records/information management personnel (or the relevant organizational charts if your public body does not have dedicated RM/IM personnel)***
- 4. Final training packages (i.e. presentation slides, etc.) and training implementation history files (e.g. reports of completion, etc.) for freedom of information and records/information management, including initial training specific to FOI analysts/coordinators.***
- 5. Internal surveys and the results of surveys concerning records/information management and freedom of information. [Date Range: 1 January 2021 to 13 August 2024]***

The records located in response to your request are attached. Some information has been withheld pursuant to section(s) 13 (Policy advice or recommendations) and 17 (Disclosure harmful to the financial or economic interests of a public body). A complete copy of FOIPPA is available online at: [Freedom of Information and Protection of Privacy Act \(gov.bc.ca\)](https://www.gov.bc.ca/freedom-of-information-and-protection-of-privacy-act).

Please note, a copy of these records will be published on the BCER's website. To find out more about proactive disclosure of requests, please access the BCER website: [foi-proactive-disclosure-policy.pdf \(bc-er.ca\)](#). Your file is now closed. Pursuant to section 52 of the FOIPPA, you may ask the Office of the Information and Privacy Commissioner (OIPC) to review any decision, act, or failure to act with regard to your request under FOIPPA within 30 business days by writing to:

*Information and Privacy Commissioner*  
*PO Box 9038 Stn Prov Govt*  
*4<sup>th</sup> Floor, 947 Fort Street*  
*Victoria BC V8W 9A4*  
*Phone: 250.387.5629 Fax: 250.387.1696 Email: [info@oipc.bc.ca](mailto:info@oipc.bc.ca)*

If you request a review, please provide the OIPC with a copy of your original request, a copy of the BCER's response, and the reasons or grounds upon which you are requesting the review. Further information on the complaint and review process can be found on the OIPC website: <https://www.oipc.bc.ca>. Please write [FOIIntake@bc-er.ca](mailto:FOIIntake@bc-er.ca), if you have any questions regarding your request or require any further clarification.

Sincerely,

*D. Keough*  
BC Energy Regulator

POSITION TITLE:	Director, Records & Information Management	POSITION #:	573798
DIVISION:	People, Reconciliation & Transformation	CLASSIFICATION:	Management Band B
Program Area:	Digital Transformation & Public Trust	LOCATION:	All BCER locations
SUPERVISOR'S TITLE:	Executive Director, Information Systems & Technology	POSITION #:	573019
SUPERVISOR'S CLASSIFICATION:	Management Band C	LOCATION:	Victoria

The BC Energy Regulator (BCER) is the Province of B.C.'s life-cycle energy resources regulator. The BCER is a Crown agency with a mandate to ensure energy resource activities are undertaken in a manner that: protects public safety and the environment, supports reconciliation with Indigenous peoples and the transition to low-carbon energy, conserves energy resources and fosters a sound economy and social well-being.

As a cost recoverable, values driven organization, we prioritize safety, stewardship and Indigenous interests throughout the full project lifecycle – from exploration to reclamation – and support the transition to clean energy. The BCER is committed to reconciliation with Indigenous Peoples, honouring the Provincial commitment to the United Nations Declaration on the Rights of Indigenous Peoples, the *Declaration on the Rights of Indigenous Peoples Act*, and the Truth and Reconciliation BCER's (TRC) Calls to Action. Through fostering respectful and collaborative relationships with Indigenous partners and stakeholders, the BCER delivers on Government's priorities.

The BCER has an innovative forward-thinking workplace that demonstrates our core values. Through continuous improvement and development, the BCER is agile and responsive to the rapidly changing environment in which we operate. We are diverse and inclusive, with transparency, innovation, and integrity as foundation of our respectful culture.

**JOB OVERVIEW**

The Director, Records & Information Management (Director) oversees the BCER's records and information management, Freedom of Information (FOI) and privacy management programs. Reporting to the Executive Director, Information Systems & Technology, the Director is responsible for developing strategic goals and objectives and implementing strategies to advance the organization towards a state of maturity and legislative compliance in each area. A key requirement of the role involves establishing effective short and long-term solutions to content management, preservation, and governance in Microsoft Office 365 (M365) as the BCER's new digital platform. Other position accountabilities include leading multiple information, privacy and digital transformation projects and participating in corporate initiatives and committees as a subject matter expert.

**ACCOUNTABILITIES**

**Leads, oversees, and manages the BCER's records and information (digital and physical) program in accordance with BC government legislation, directives, and standards:**

- Provides strategic direction and advice to ensure the organization is fully compliant with all legislative information management requirements.
- Develops and implements strategies, policies, and processes to ensure compliant management and retention of content created and maintained in M365 applications (e.g., Teams, OneDrive and SharePoint) and BCER systems.

- Actively supports the planning, design, configuration and maintenance of M365 SharePoint sites as compliant records management/ECM solutions for BCER departments.
- Leads digital transformation and other related projects to improve access, preservation and ongoing management of BCER information.
- Supports organizational change management and facilitates employee training initiatives.
- Develops and implements information schedules to enable lifecycle management and disposition in accordance with the Information Management Act and related policies.
- Oversees corporate information disposition processes (digital and physical).
- Champions data stewardship and information governance practices.
- Implements client service delivery model improvements through policy, process and/or technological enhancements.
- Liaises with other government agencies on best practices and technological solutions.
- Collaborates with various departments and stakeholders, such as legal, Information Systems, Architecture and Innovation, and business units, to ensure alignment and integration of records and information management practices across the organization. Builds relationships and promotes a culture of cooperation and engagement.
- Assesses, supports the implementation, and maintaining of records management systems and technologies that enable efficient and secure management of records and information. This involves evaluating the organization's technological needs, selecting appropriate tools, and integrating them with existing systems.

**Leads the administration and application of the Freedom of Information and Protection of Privacy Act (FOIPPA) across the organization:**

- Oversees the administration of Freedom of Information (FOI) requests and proactive release of BCER information.
- Develops, implements, and maintains the BCER's Privacy Management Program as issued under FOIPPA s.36.2, including but not limited to oversight of breach response protocols and privacy impact assessments.
- Ensures information, policies and procedures related to FOI and privacy protection are readily available to BCER employees.
- Works collaboratively with employees, service providers, and other public bodies to build privacy protection into business activities involving the collection, use and/or disclosure of personal information.
- Prepares reports, briefing notes, and Estimates materials as required for supervisor and Executive.

**Leads the Records and Information Services (RIS) Branch:**

- Builds branch competencies, expertise, capacity, and overall organizational knowledge in relation to records and information management, Freedom of Information (FOI) and privacy.

**ORGANIZATION CHART**

Commissioner, Chief Executive Officer

Executive Vice President, People, Reconciliation & Transformation

Vice President, Digital Transformation & Public Trust

Executive Director, Information Systems & Technology

***Director, Records & Information Management (TOPIC POSITION)***

**EDUCATION AND EXPERIENCE REQUIREMENTS**

**Education:**

- Degree in Library and Information Studies, Information Management, Archival Studies, Business or Public Administration, or other related field, and a minimum of 7 years of professional information management experience in records and information management and information access in a provincial government setting, or an equivalent combination of education and minimum of 10 years related experience.

**Experience:**

- Demonstrated experience in a management role leading a records and information management program within a public sector setting.
- Experience leading new business development initiatives and/or digital transformation projects.

- Experience in supporting multiple clients in a diverse range of project portfolios, in a customer service environment.
- Demonstrated experience working in a project management and/or change management leadership role.
- Demonstrated experience supervising staff and/or contractors.
- Experience interpreting and applying BC legislation and government policies related to records and information management.
- Experience in developing and implementing records classification (information) schedules.
- Experience applying information lifecycle management and disposition processes (digital and physical records).
- Experience developing and delivering effective training to management and other levels of staff on information management requirements, principles and best practices.
- Strong working knowledge and understanding of electronic document and records management systems (EDRMS).
- Strong knowledge and experience using Microsoft Office 365 (M365) Teams, OneDrive and SharePoint and the application of records management functionality.
- Knowledge and experience in the application of the Freedom of Information and Protection of Privacy Act (FOIPPA) and Information Management Act (IMA).
- Experience reviewing and/or completing privacy impact assessments.
- Experience managing programs or providing specified knowledge in the area of natural resources, business management, or oil and gas industry operations.

#### **FINANCIAL RESPONSIBILITIES**

- Responsible for the Records & Information Services Branch operational budget and capital costs associated with transformation initiatives.

#### **KEY COMPETENCIES**

**Leadership** - implies a desire to lead others, including diverse teams

**Developing Others** - involves a genuine intent to foster the long-term learning or development of others through coaching, managing performance and mentoring

**Results Orientation** - is a concern for surpassing a standard of excellence (striving for improvement, achievement, continuous improvement)

**Managing Organization Resources** - is the ability to understand and effectively manage organizational resources (e.g. people, materials, assets, budgets)

**Teamwork and Cooperation** - is the ability to work co-operatively within diverse teams, work groups and across the organization to achieve group and organizational goals. It includes the desire and ability to understand and respond effectively to other people from diverse backgrounds with diverse views.

**Analytical Thinking** - is the ability to comprehend a situation by breaking it down into its components and identifying key or underlying complex issues. It implies the ability to systematically organize and compare the various aspects of a problem or situation, and determine cause-and-effect relationships (“if...then...”) to resolve problems in a sound, decisive manner. Checks to ensure the validity or accuracy of all information.

POSITION TITLE	Specialist, FOIPP & Information Management	POSITION #:	573847
DIVISION	Corporate Services	LOCATION:	Victoria
PROGRAM:	Records Management	CLASSIFICATION	Grid 27
SUPERVISOR'S TITLE:	Director, Records & Information Management	POSITION #:	573798
SUPERVISOR'S CLASSIFICATION:	Band B	LOCATION:	Victoria

The BC Oil and Gas Commission (Commission) is an independent, single-window regulatory agency with responsibilities for regulating oil and gas operations in British Columbia, including exploration, development, pipeline transportation and reclamation. The Commission's core roles include reviewing and assessing applications for industry activity, consulting with First Nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected through the objectives of ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

**Job Overview**

Reporting to the Director, Records & Information Management, the Specialist, FOIPP & Information Management supports the Commission in meeting its legal obligations under the Freedom of Information and Protection of Privacy Act (FOIPPA) and Information Management Act (IMA) through the daily management and administration of Freedom of Information (FOI), proactive release, document discovery, privacy compliance, and information management services.

This position exercises considerable independence, discretion and sound judgement in managing these services on behalf of the Commission. The Specialist supports the Director in achieving strategic goals, corporate objectives and performance targets, and adhering to rigid timelines (legislative and otherwise). In an environment of increasing legislative changes and challenges involving electronic information management, this position works to develop solutions and foster best practices. Diplomatic and service-focused, this position provides expert leadership, strategic advice, mentoring, guidance, training, and support services to Commission employees in helping them understand and meet their accountabilities under FOIPPA and the IMA. This positions supervises at least one unionized position.

**Accountabilities**

**1. Freedom of Information (FOI), Proactive Release and Litigation**

- Manages the Commission's FOIPPA Program;
- Manages all processes associated with the Office of the Information and Privacy Commissioner (OIPC) reviews of complaints, mediation and inquiries, plus litigation document discovery searches and investigations by the Ombudsperson;
- Provides strategic advice and direction to the Commission's Executive, Leadership Group and internal clients on the legislated obligations of FOIPPA as it relates to information access requests (FOI requests) and proactive information releases;
- Manages the internal FOI review, approval, sign-off and release process;
- Implements and manages internal performance standards for FOI administration aligned with legislated requirements and Commission policy and procedures, to ensure FOIPP Program delivery objectives and legal requirements are being appropriately met;
- Develops, implements and manages an internal FOI audit system to measure and evaluate corporate compliance with statutory obligations and Commission objectives, policies and procedures.
- Reviews all requested records for harms prior to release (under FOI or through proactive disclosure), and provides expert advice and direction on the application of FOIPPA to ensure compliance and mitigate risks associated with sensitive issues;

- Leads the development of new internal tracking and reporting systems to effectively manage requests, identify risks or issues, and support Executive reporting and briefings, and corporate statistical requirements;
- Acts in the capacity of the Director, Records and Information Management as and when required for FOIPPA related matters.
- Provides leadership in terms of FOIPPA initiatives, including policy and procedure development, staff training (informal and formal), and other information dissemination initiatives;
- Leads or represents the Commission on inter-governmental committees, working groups and initiatives and represents the RIM business unit on Commission committees, as required.
- Supervises staff by assigning and reviewing work, developing and evaluating performance plans (EPDP's), evaluating work performance, approving leave, responding to grievances, and taking disciplinary action as required; and
- Manages and coordinates the litigation document discovery process for legal matters, as required

## 2. Privacy

- Leads the establishment of an internal privacy program;
- Develops privacy assessment frameworks for the translation of government's privacy requirements into viable policy, procedural or program changes;
- Manages the completion of Privacy Impact Assessments (PIAs) on new and/or updated corporate programs, legislation, initiatives and systems, as applicable;
- Provides advice on operational privacy matters and mitigation strategies;

## 3. Information Management (IM)

- Supports the Director in planning and implementing priority activities associated with Commission's long-term IM strategy and legislated accountabilities under the IMA;
- Identifies opportunities to reduce costs, streamline processes, support business needs, and improve stakeholder satisfaction;
- Monitors and assesses internal practices to ensure corporate information is managed in accordance with FOIPPA and other relevant legislation and policies addressing the management of information and records;
- Assists program areas with specific records projects and objectives;
- Provides advice, guidance and day-to-day support to staff on records and information management policies, procedures and standards;
- Develops communications, procedures, methodologies, reports, training materials, presentations and tools for use in projects and initiatives; and
- Delivers training and education to Commission employees.

### Organization Chart

Commissioner, Chief Executive Officer

Executive Vice President, Chief Financial Officer

Executive Director, Finance & Administration

Director, Records & Information Management

**Specialist, FOIPP & Information Management**

### Education:

Degree in Library and Information Studies, Information management, Archival Studies, Business or Public Administration, Education, or an equivalent combination of training and work experience; and a minimum of 3 consecutive years of experience administering requests for information under the Freedom of Information and Protection of Privacy Act.

### Related Experience:

- Proven experience in the interpretation and application of FOIPPA for access to information (FOI) request processing.
- Experience managing a portfolio of clients in customer service environment with the ability to use tact, diplomacy and sensitivity in handling confidential information, communicating with the public, and working with internal staff on complicated and/or sensitive issues.
- Experience providing advice on policy, procedures and guidelines to staff at all levels.
- Experience establishing, managing or maintaining a records program within a government setting.
- Experience using government records management systems (e.g. TRIM).
- Experience in leading projects and project management.
- Experience in facilitating related training.
- Experience researching/searching, analyzing, and compiling detailed information or reports.
- Experience in managing a diverse and fluctuating workload

## Competencies

**Service Orientation** - Takes personal responsibility for addressing client questions and concerns

**Detail Oriented** - Sets and attains high standards for quality and accuracy in work

**Initiative** - Takes the initiative to identify new challenges or opportunities

**Process Improvement** - Proactively identifies process improvements and takes the appropriate steps to implement them

**Problem Solving** - Uses critical thinking skills to solve problems and achieve effective solutions

**Communication** - Ability to clearly convey and receive messages

**Teamwork** - Working cooperatively and productively with others to achieve results

**Focus on Priorities** - Is able to identify priority activities and remains focussed on the highest priorities



POSITION TITLE:	Specialist, Digital Information Management	POSITION #:	573861
DIVISION:	People, Reconciliation & Transformation	CLASSIFICATION:	Grid 27
Program Area:	Records & Information Services	LOCATION:	Victoria/Fort St John
SUPERVISOR'S TITLE:	Director, Records & Information Management	POSITION #:	573798
SUPERVISOR'S CLASSIFICATION:	Band B	LOCATION:	Victoria

The BC Energy Regulator (BCER) is the Province of B.C.'s life-cycle energy resources regulator. The BCER is a Crown agency with a mandate to ensure energy resource activities are undertaken in a manner that: protects public safety and the environment, supports reconciliation with Indigenous peoples and the transition to low-carbon energy, conserves energy resources and fosters a sound economy and social well-being.

As a cost recoverable, values driven organization, we prioritize safety, stewardship, and Indigenous interests throughout the full project lifecycle – from exploration to reclamation – and support the transition to clean energy. The BCER is committed to reconciliation with Indigenous Peoples, honouring the Provincial commitment to the United Nations Declaration on the Rights of Indigenous Peoples, the *Declaration on the Rights of Indigenous Peoples Act*, and the Truth and Reconciliation Commission (TRC) Calls to Action. Through fostering respectful and collaborative relationships with Indigenous partners and stakeholders, the BCER delivers on Government's priorities.

The BCER has an innovative forward-thinking workplace that demonstrates our core values. Through continuous improvement and development, the BCER is agile and responsive to the rapidly changing environment in which we operate. We are diverse and inclusive, with transparency, innovation, and integrity as foundation of our respectful culture.

**JOB OVERVIEW**

The Records & Information Services branch supports the BCER in meeting its mandate and legal obligations in the areas of records management, access, and privacy in accordance with the *Information Management Act (IMA)*, *Professional Governance Act (PGA)*, *Freedom of Information and Protection of Privacy Act (FOIPPA)*, and other applicable legislation.

The Specialist, Digital Information Management (Specialist) guides the short and longer-term development, implementation, and maintenance of the corporate records management initiatives with a focus on Microsoft Office 365 (M365) and its technologies. As leader of the Digital Information Management Program, the Specialist provides policy and technical advice to ensure records management policy is upheld; ensures legal and regulatory requirements are adequately met in the M365 environment; oversees the design of departmental SharePoint sites to ensure appropriate management and retention of corporate information; and offers change management support; develops and maintains positive working relationships throughout the BCER; and champions and promotes a strong records management culture and the benefit of mature information management practices.

As a subject matter expert, the Specialist exercises a high degree of independence, discretion, and sound judgement while influencing necessary improvements and changes to digital information governance for the BCER.

## ACCOUNTABILITIES

- Develops and implements policy and procedures for records management statutory compliance across the organization particularly within cloud-based solutions, including M365 and its applications.
- Serves in multiple project leadership and management roles to support digital information management program initiatives and adoption of M365 applications.
- Works directly with stakeholders to identify records management business requirements and ensures their translation into information systems and M365 SharePoint design.
- Manages contractors and monitors deliverables to ensure service quality, and delivery on budget within established timelines.
- Leads the design and delivery of corporate-wide training programs on records management compliance and best practices.
- Develops and identifies objectives, targets, and performance measures for records management compliance.
- Provides advice and direction to BCER management and staff regarding information management issues and concerns and participates in planning processes for their resolution.
- Develops and/or facilitates the amendment and approval process of the BCER's Information Schedule (Operational Records Classification System [ORCS]).
- Conducts records management assessments as part of the BCER's Privacy Impact Assessment (PIA) process.
- Supervises and supports records management staff as applicable, by assigning projects and tasks, setting priorities or goals, mentoring and training, approving leave, etc.
- Acts in the role of branch Director, reports to Executive and Leadership, and represents the BCER in external committees and working groups, as required.

## ORGANIZATION CHART

Commissioner, Chief Executive Officer

Executive Vice President, People, Reconciliation & Transformation

Vice President, Digital Transformation & Public Trust

Executive Director, Information Systems & Technology

Director, Records & Information Management

***Specialist, Digital Information Management (Topic Position)***

## EDUCATION AND EXPERIENCE REQUIREMENTS

### Education:

- Bachelor's degree in Library & Information Studies, Information Management, Archival Studies, Business, Public Administration and 3 years related experience; or,
- An equivalent combination of education, training and experience.

### Experience:

- Direct experience with Microsoft Office 365 and SharePoint/Purview as a digital records repository.
- Direct experience with Electronic Document and Records Management Systems (EDRMS).
- Advanced knowledge of BC provincial government records management policy, procedures, and legislation.
- Experience leading complex, large-scale and time-sensitive projects and managing a portfolio of clients.
- Knowledge of change management processes and project management methodologies.
- Experience establishing collaborative relationships with senior management and leading organizational change.
- Proven experience in developing Information Schedules (ORCS) and data retention plans for information system overviews.
- Experience in facilitating training and providing corporate direction on policies, procedures, and legislated requirements.
- Experience and ability to use tact, diplomacy, and sensitivity in handling confidential information and issues.
- Experience in managing a diverse and fluctuating workload.

## KEY COMPETENCIES

**Service Orientation** – Takes personal responsibility for addressing client questions and concerns.

**Teamwork & Cooperation** – Is able to work cooperatively within diverse teams, work groups and across the Regulator to achieve operational goals and results.

**Problem Solving** – Uses critical thinking skills to solve problems and achieve effective solutions.

**Communicates Strategy & Rationale** – Is able to effectively communicate vision and rationale behind decisions and policies.

POSITION TITLE:	Records & Information Management Analyst	POSITION #: 573247	
DIVISION:	Corporate Services	CLASSIFICATION: Grid 15	
Program Area:	Records & Information Management	LOCATION: Victoria	
SUPERVISOR'S TITLE:	Specialist, EDRMS & Info Management Solutions	POSITION #: 573861	
SUPERVISOR'S CLASSIFICATION:	Grid 24	LOCATION: Victoria	

The BC Oil and Gas Commission (Commission) is an independent, single-window regulatory agency with responsibilities for regulating oil and gas operations in British Columbia, including exploration, development, pipeline transportation and reclamation.

The Commission's core roles include reviewing and assessing applications for industry activity, consulting with First Nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected through the objectives of ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

### **JOB OVERVIEW**

The BC Government's information management landscape is undergoing modernization and significantly transforming the way that public bodies must manage their recorded information, with heightened focus on compliance, digitization/electronic records management, and alignment with Government's commitment to openness and transparency. The Records and Information Management (RIM) unit provides leadership, direction and support to the Commission in meeting new legal requirements for electronic information management under the new *Information Management Act (IMA)*, and information access and privacy protection obligations in accordance with *The Freedom of Information and Protection of Privacy Act (FOIPPA)*.

The Records and Information Management (RIM) Analyst is a key member of the Commission's Records and Information Management (RIM) business unit. Under the direction of the RIM Director, this position is responsible for a broad range of records and information management (RIM) functions focused on achieving legislative compliance, promoting best practices, mitigating risks, improving operational efficiency, and developing customized solutions to RIM challenges to effect positive change and support the availability, integrity, accuracy and effective management of client information assets.

### **ACCOUNTABILITIES**

- Provides advice to a diverse corporate client base on the interpretation, application and impact of BC's new Information Management Act (IMA), and government's supporting policies, standards and procedures.
- Takes a leading role within the Commission to promote awareness and understanding of the changing landscape of recorded information management under the IMA (electronic/digital information management and change management focus).
- Leads clients towards finding appropriate solutions to challenges related to managing electronic data/information by developing, implementing and/or guiding the implementation of electronic file plans and document naming conventions for shared network folders and documents, and for application within data systems.

- Contributes to the ongoing testing and improvement of corporate information systems (e.g. IRIS, Kermit) and provides feedback to database developer(s) with respect to data issues, upload/download activities, etc. to support positive user experiences and functional efficiency.
- Applies expert knowledge of digital records management applications and technology, and industry-approved standards for digitization of Commission original physical records.
- Analyzes and reviews oil and gas industry data types (such as LAS, XML and PAS files) and other digital data for quality/integrity/standards/issues prior to external publishing to e-Library and/or applicable FTP sites in support of the Business Transformation Strategy (BTS) and other proactive release requirements.
- Provides project management leadership and/or support to client information management projects, ensuring Commission information assets are managed effectively in accordance with their value and as required by current legislation, policy, standards and procedures.
- Identifies information, communication and training needs to develop resources, educational materials and communication tools, including web content for intranet and extranet sites.
- Develops and delivers and/or assists in the delivery of records and information management training.
- Contributes to the development of disaster preparedness and recovery plans.
- Researches policy developments and best practices on the management of digital information, and recommends enhancements to current policies and procedures as corporate business functions, legislation or government-wide policies and procedures are introduced or amended.
- Researches oil and gas industry (e.g. well, field and pool, etc.) legislation, regulations, policy and procedures as they apply to external stakeholder inquiries and requests.
- Provides input to the development of new corporate records and information management policy.
- Provides expert advice and guidance to internal clients on a daily basis about the classification, creation, retention, retrieval and disposition of records and data in accordance with ARCS and ORCS.
- As a first point of contact for information requests from industry/external stakeholders, provides expert support for service desk requests involving complex and high volume data searches and/or troubleshooting and time-sensitive issues.
- Interprets and effectively responds to issues, queries and requests for information from internal and external client stakeholder groups through a range of communication channels, ensuring corporate service standards for timeliness, prioritization, accuracy, and quality of response are achieved.
- Using expert knowledge of Commission operational records, RIM best practices and confidentiality principles applied to corporate records and business data, reviews requested information prior to release to prevent risks associated with unauthorized disclosure.
- Conducts audits and reviews to assess compliance on records and information management practices and processes, and develops recommendations for improving efficiency and reducing risk.
- Applies business and records management knowledge to contribute to the development and review of the Commission's Operational Records Classification System (ORCS).
- Approves disposition (including destruction or preservation) of non-transitory scheduled client recorded information as the Commission's alternate Corporate Records Officer.
- Monitors, tracks and reports on expenditures, progress, and timelines related to RIM contracts and projects and storage, imaging, and disposal services, as required.
- Establishes and maintains multiple, complex registries of active and semi-active corporate record holdings stored onsite, or in various government-contracted location and Commission offices/facilities.

## **ORGANIZATION CHART**

Commissioner, Chief Executive Officer

Executive Vice President, Chief Financial Officer

Executive Director, Finance and Administration

Director, Records & Information Management

Specialist, EDRMS & Info Management Solutions

Records & Information Management Analyst (Topic Position)

## EDUCATION AND EXPERIENCE REQUIREMENTS

### Education:

High school diploma supplemented with post-secondary courses in records management, archival studies, business or public administration plus three years of related experience.; OR technical diploma in records management, archival studies or closely related discipline and two years of related experience; OR degree in library or archival studies, business, public administration, management and one year of related experience.

### Experience:

- Progressive experience in data, document and information management (e.g. classification, scheduling, transfers and retrievals, disposition, digitization/imaging technology, governing legislation, technical standards, etc.).
- Experience in providing on-going advice and guidance to staff of all levels on records management policies, procedures, standards and best practices.
- Ability to liaise effectively with internal and external stakeholders, such as internal business groups and members of the oil and gas industry.
- Experience in managing administrative and operational records in various formats according to ARCS and ORCS and/or approved records schedules.
- Experience with managing projects, including providing technical direction to staff.
- Demonstrated experience and ability to organize, manage and complete a number of concurrent projects.
- Strong ability to demonstrate tact, discretion, and sensitivity when dealing with clients, stakeholders, sensitive situations and confidential material.
- Ability to maintain strict confidentiality.
- Ability to ensure a high standard of accuracy in all levels of work.
- Ability to work independently or in a team environment, under significant pressure and meet deadlines.

### Knowledge:

- BC Information Management Act (IMA) and associated policies and procedures
- BC Government Records and Information Management Manual
- BC Government Administrative Records Classification System (ARCS) and BC Oil and Gas Commission's Operational Records Classification System (ORCS)
- Commission policies, procedures and guidelines relating to records and information management, eSubmission and oil and gas activities.
- Oil and Gas Activities Act (OGAA) and other related sector legislation and regulations.

## KEY COMPETENCIES

**Service Orientation** - Takes personal responsibility for addressing client questions and concerns

**Detail Oriented** - Sets and attains high standards for quality and accuracy in work

**Initiative** - Takes the initiative to identify new challenges or opportunities

**Process Improvement** - Proactively identifies process improvements and takes the appropriate steps to implement them

**Problem Solving** - Uses critical thinking skills to solve problems and achieve effective solutions

**Communication** - Ability to clearly convey and receive messages

**Adaptability** - Willingness and ability to effectively work in and adapt to change

**Teamwork** - Working cooperatively and productively with others to achieve results

**Focus on Priorities** - Is able to identify priority activities and remains focused on the highest priorities

POSITION TITLE:	Well File Technician	POSITION #:	573268
DIVISION:	Corporate Services	CLASSIFICATION:	Grid 15
Program Area:	Finance and Administration	LOCATION:	Victoria
SUPERVISOR'S TITLE:	Specialist FOIPP and Information Management	POSITION #:	573847
SUPERVISOR'S CLASSIFICATION:	Grid 27	LOCATION:	Fort St. John

The BC Oil and Gas Commission (Commission) is the provincial single-window regulatory agency with responsibilities for regulating oil and gas operations in British Columbia, including exploration, development, pipeline transportation and reclamation.

The Commission's core roles include reviewing and assessing applications for industry activity, consulting with First Nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected through the objectives of ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

**JOB OVERVIEW**

The principal functions of the Well File Technician are to provide expert administration and management of technical well data including ensuring industry compliance with regulations and guidelines, coordination of the public release of data from confidential status, and the development, implementation and management of all aspects of best practices and procedures relating to well data document management. The position contributes to the management and exploration of the Province's petroleum and natural gas operations by responding to industry queries regarding well data. The position also oversees the categorization, recording and tracking of all incoming technical well data using a complex document management system, and manages staff to carry this out.

**ACCOUNTABILITIES**

- Responsible for compliance to ensure that required data is submitted in the formats and timeframes stipulated by regulation and OGC guidelines, and contributes to the development of those guidelines;
- Interprets regulations and develops guidelines for compliance of well data submissions;
- Develops, implements and maintains procedures and processes in accordance with generally accepted Document Management best practices, applying document management expertise relating to all aspects well data document management including but not limited to document processing, submission requirements, compliance and enforcement, scanning and imaging, etc.;
- Responsible for the implementation of the scanning and imaging of well data and logs and the overseeing of the scanning well data and logs into appropriate electronic applications;
- Coordinates the timely review, recording, approval and communication for all core and sample removal applications. Carries out the designated OGAA approval where applicable;
- Oversees the categorization, recording and tracking of all incoming technical well data, including the transfer of digital data into appropriate locations;
- Responds to enquiries from Canadian Association of Petroleum Producers (CAPP), Canadian Association of Petroleum Information Specialists (CAPIS) and other petroleum data vendors regarding information pertinent to the oil & gas exploration activities in British Columbia;



- Researches, plans, develops, and implements consistent Records Management Functions across worksites;
- Develops the procedures / processes to bring the OGC up to current recognized best practices in order to ensure the completeness of the well files and that the information captured is reliable and accessible over time and location.

**ORGANIZATION CHART**

Commissioner, Chief Executive Officer  
 Executive Vice President, Chief Financial Officer  
 Executive Director, Finance and Administration  
 Director, Records and Information Management  
 Specialist, FOIPP and Information Management  
**Well File Technician (Topic Position)**

**EDUCATION AND EXPERIENCE REQUIREMENTS**

**Education:**

- High school diploma supplemented with post secondary courses in records management, archival studies, business or public administration plus 3 years of related experience.; OR
- Technical diploma in records management, archival studies or closely related discipline and 2 years of related experience; OR
- Bachelor’s degree in library or archival studies, business, public administration, management and 1 year of related experience;
- There will be different combinations of relevant experience, education and/or training that would result in an applicant meeting the above standards.

**Experience:**

- Progressive experience in document management, records management and scanning and imaging;
- Must have established, guided and provided on-going advice regarding the records and document management and the scheduling of records which ensures systematic organization, retrieval, storage, destruction or permanent destruction;
- Management of administrative and operations records including paper files, microfilm, diskettes, magnetic tape, electronic data processing records, and video or audiotapes; and
- Supervising staff.

**KEY COMPETENCIES**

**Service Orientation** - displaying a desire to identify and serve customers/clients, who may include the public, colleagues, partners (e.g. educational institutes, non-government organizations, etc.), co-workers, peers, branches, ministries/agencies and other government organizations and focusing one's efforts on discovering and meeting the needs of such customers/clients.

**Results Orientation** - showing concern for surpassing a standard of excellence, be it one's own past performance (striving for improvement); an objective measure (achievement orientation); challenging goals one has set; or even improving or surpassing what has already been done (continuous improvement).

**Teamwork and Cooperation** - demonstrates the ability to work co-operatively within diverse teams, work groups and across the organization to achieve group and organizational goals.

**Concern for Order** - reflects an underlying drive to reduce uncertainty in the surrounding environment. It is expressed as monitoring and checking work or information, insisting on clarity of roles and functions, etc.

---

DATE

---

EXCLUDED MANAGER SIGNATURE



POSITION TITLE:	Records Coordinator	POSITION #:	573906/573907
DIVISION:	People, Reconciliation & Transformation	CLASSIFICATION:	Grid 12
PROGRAM AREA:	Records & Information Services	LOCATION:	Fort St. John
SUPERVISOR'S TITLE:	Specialist, FOIPP & Information Management	POSITION #:	573847
SUPERVISOR'S CLASSIFICATION:	Grid 27	LOCATION:	Fort St. John

The BC Energy Regulator (BCER) is the Province of B.C.'s life-cycle energy resources regulator. The BCER is a Crown agency with a mandate to ensure energy resource activities are undertaken in a manner that: protects public safety and the environment, supports reconciliation with Indigenous peoples and the transition to low-carbon energy, conserves energy resources and fosters a sound economy and social well-being.

As a cost recoverable, values driven organization, we prioritize safety, stewardship and Indigenous interests throughout the full project lifecycle – from exploration to reclamation – and support the transition to clean energy. The BCER is committed to reconciliation with Indigenous Peoples, honouring the Provincial commitment to the United Nations Declaration on the Rights of Indigenous Peoples, the *Declaration on the Rights of Indigenous Peoples Act*, and the Truth and Reconciliation BCER's (TRC) Calls to Action. Through fostering respectful and collaborative relationships with Indigenous partners and stakeholders, the BCER delivers on Government's priorities.

The BCER has an innovative forward-thinking workplace that demonstrates our core values. Through continuous improvement and development, the BCER is agile and responsive to the rapidly changing environment in which we operate. We are diverse and inclusive, with transparency, innovation, and integrity as foundation of our respectful culture.

### **JOB OVERVIEW**

The Records Coordinator (Coordinator) provides hands-on support in the Records & Information Services Branch. Under the direction of the Specialist, FOIPP, this role is responsible for coordinating and maintaining the storage, access, use, and disclosure of BCER records, both electronic and paper. The Coordinator responds to requests for records and information received from internal and external stakeholders, by locating and digitizing (scanning) a high volume of paper files and documents in a timely manner. This role provides exceptional customer service in a busy environment while dealing with a variety of confidential and sensitive materials. This position also provides back-up coverage for the Receptionist in the Fort St. John office when required.

### **ACCOUNTABILITIES**

- Maintains the efficient operation of the Fort St. John Records Centre on a day-to-day basis by ensuring BCER files and documents are appropriately maintained in accordance with established best practices. This includes:
  - Filing, classifying, organizing, putting into inventory, and culling records in accordance with ARCS and ORCS retention schedules, and government standards.
  - Responding to a high volume of time sensitive requests and correspondence as the first point of contact.
  - Interpreting client requests for copies of BCER records and responding with speed and accuracy, in accordance with applicable policies, procedures, and legislation.
  - Understanding of requests and data retrieval actions required as related to Freedom of Information and legalities of request.

- Applying a sound understanding of BCER records, recordkeeping systems, and information systems to ensure accurate and complete responses.
- Reviewing requested information prior to release and making appropriate decisions on withholding personal and/or confidential information from disclosure in accordance with the Freedom of Information and Protection of Privacy Act (FOIPPA) exceptions to disclosure.
- Providing on site coordination and support for records access and digitization activities to external clients and/or contractors as required.
- Works with scanners/imaging equipment to convert high volumes of paper records into digital copies in accordance with established standards.
- Applies technical skills and a knowledge of BCER systems (IRIS, Kermit, AMS, FTP sites, Service Desk, etc.) to efficiently search/locate, copy, download, consolidate, and release electronic records in response to requests.
- Provides back-up coverage for the Fort St. John office Receptionist position as and when needed; coverage may include receiving, screening and appropriately directing incoming calls, greeting walk-in clients and visitors, coordinating mail/courier services, and assisting with boardroom bookings.
- Establishes, maintains, and promotes positive relationships with BCER staff, clients, and external stakeholders.
- Performs other related duties required or assigned.

## **ORGANIZATION CHART**

Commissioner, Chief Executive Officer

Executive Vice President, People, Reconciliation & Transformation

Vice President, Digital Transformation & Public Trust

Executive Director, Information Systems & Technology

Director, Records & Information Management

Specialist, FOIPP & Information Management

**Records Coordinator (*Topic Position*)**

## **EDUCATION AND EXPERIENCE REQUIREMENTS**

### **Education:**

- Completion of Grade 12 or equivalent, supplemented with courses in records management; archival studies, business, or library sciences plus two or more years of related experience; *OR*
- Technical diploma in records management, archival studies or closely related discipline and two years of related experience; *OR*
- A combination of three years of administrative support experience, education and/or training.

### **Experience:**

- Demonstrated experience working with a recordkeeping or filing system for paper and/or electronic records where best practices were applied. Preference to candidates with knowledge of records management best practices as it applies to BC public bodies and ARCS/ORCS.
- Demonstrated ability to interpret policies and follow standard procedures.
- Experience with Microsoft Office products and using a range of information systems.
- Experience in managing and prioritizing multiple work tasks in a high-pressure setting, while exercising a high degree of accuracy and professionalism.
- Experience working in a customer service-focused environment and providing excellent service levels.
- Demonstrated ability to act in a professional and respectful manner and contribute to a positive work environment.

***\*Given the nature of this position, it is required to work in the Hub Office. Must be able to lift up to 30 lbs***

## **KEY COMPETENCIES**

**Communication** - Ability to clearly convey and receive messages

**Teamwork** - Working cooperatively and productively with others to achieve results

**Service Orientation** - Takes personal responsibility for addressing client questions and concerns

**Detail Oriented** - Sets and attains high standards for quality and accuracy in work

# Information Management Foundations



Welcome to the Information Management Foundations eLearning course. This course will familiarize you with the basics of information management, including an understanding of:

- What government information is;
- Your FOIPPA responsibilities; and
- Privacy awareness

St. Mark's Summit, West Vancouver

## Adventures in...



## Records Management

The BC Energy Regulator (BCER) is the steward of a significant amount of government information, and we all have an important role in creating a culture of efficient and effective information management. This section provides guidance about information management obligations and best practices that are essential to the work of all BCER employees.

Upon completion of this topic, learners will be able to:

- Understand what government information is, and the value of records and data
- Describe the benefits of good record keeping practices
- Know their responsibilities to maintain evidence of business activities, transactions and decisions
- Recognize which records are transitory and the information schedules available for managing records
- Apply best practices around the management of records, including email

[Show less](#)

START MODULE



## Privacy

What are our responsibilities as public servants when it comes to the personal information that we hold? This section provides principles and guidance that will help us treat personal information responsibly and lawfully.

Upon completion of this topic, learners will be able to:

- Understand what personal information is
- Apply privacy principles to the work of the BCER
- Know how to identify and respond to an information incident

- Find privacy resources such as the Privacy Impact Assessment template and Guideline

Show less

START MODULE



## Access to Information

The Freedom of Information and Protection of Privacy Act (FOIPPA) provides individuals a right to access their own personal information held by public bodies, as well as general information about BCER operations, programs and services – with limited exceptions. This section describes the formal “FOI” process, as well as the proactive disclosure of government information outside of the FOI process.

Upon completion of this topic, learners will be able to:

- Recognize the obligations placed on public servants when responding to FOI requests
- Understand the roles and responsibilities of everyone involved in a FOI request
- Know how to perform an adequate search for records
- Differentiate between a FOI request and proactive disclosure

Show less

START MODULE



Contact Records and Information Services

This learning program is adapted from BC Governments IM117 course.





# Records Management

## What is government information?

Let's start with defining our terms: what do we mean by 'government information'?

Government information is recorded information in any format that is created or received by a government body (BCER) in connection with government business, including data and records. In this learning program, the term 'government information' applies to information we hold in the BCER. It is the official and legal term for the information the BCER uses, creates and receives in the course of our day.

### Records – What is Government Information?

Identify which of the following may contain government information.

**Select all that apply:**

- Case management system entries
- Voicemail messages
- MS Teams chats
- Instant messages
- Handwritten notes
- Reports
- Email messages
- Maps
- Policies
- Statistical data

**SUBMIT**

[DOWNLOAD WHAT IS GOVERNMENT INFORMATION ACTIVITY DESCRIPTION](#)

All employees are required to manage BCER information according to information schedules, relevant policies, and legislation. There are many recordkeeping practices that can be applied every day. In this section, we'll cover the basics, and good practices you need to know.

[See here](#) for a glossary of records management definitions.

## Why do we create records?

The information we create and receive is fundamental to good government and accountable public administration. Adequate records and reliable practices support efficiency and the delivery of quality services. Records and data are enterprise assets that must be managed according to their value.

They can have different values:

- Administrative
- Operational
- Evidential
- Legal
- Informational
- Financial and audit
- Historical

We rely on records every day to support the work we do. They may document key decisions and they require our care and attention.

Please keep in mind that when you're at work, you might also create or receive information that is not related to your work. Keep this information to a minimum and separate from BCER information.

Exercise: Take a minute to consider the records you interact with during your everyday work. Who relies on the information in those records? Do you understand their impact on individuals and society? And where are they kept?

## What is our framework for managing records?

To understand the framework for managing records, we need to be aware of current and updated legislation and policy, as well as standards, guides, and resources. Let's introduce some of the key parts of our framework.

The [Information Management Act](#) (IMA) is government's primary information management law, and applies to the BC Energy Regulator.



What does the IMA do? The IMA is the Province's legislative framework for digital information practices. It modernizes and streamlines government information management by:

- Transitioning government to the digital storage and management of information
- Establishing digital archives and requiring the archiving of information in digital form (subject to reasonable exceptions)
- Establishing a Chief Records Officer to approve information schedules, manage the digital archives and to promote effective information management across government
- Establishing an obligation to ensure that an appropriate system is in place to create adequate records of government decisions, and to manage and secure all government information from creation to disposal or archiving

In short, the IMA supports productivity, cost reduction, timelier services for the people of British Columbia, and improved access to information.

The BCER's [Information Management Policy](#) helps staff understand their information management (IM) obligations as they relate to IMA requirements. Policy requirements are established for the full lifecycle of information. We recommend staff read this policy.

## The information lifecycle

The information life cycle is the life span of a record from its creation or receipt to its final disposition. A record's lifecycle includes three main phases: active, semi-active, and final disposition. During this life cycle a record may be created, received, classified, scheduled, maintained, used, stored, destroyed and/or transferred for permanent retention in the government archives.

### Records: The Information lifecycle

Which term accurately describes these common office activities.  
Drag the applicable description on the top to the correct term.

Documenting a key decision

Destruction

Creation

Receipt

Classification

Maintenance



[DOWNLOAD THE INFORMATION LIFECYCLE ACTIVITY DESCRIPTION](#)

### Documenting decisions

You must take reasonable steps to ensure that adequate records of decisions are created and maintained.

It's important that the Regulator manages information so it's reliable and available to those who need it, and to ensure that it's kept for the required length of time.

The IMA establishes an obligation to ensure that an appropriate system is in place to create adequate records of government decisions. Under the IMA, the Chief Records Officer has issued a directive and guidelines to assist government bodies in meeting their obligations related to documenting their decisions.

In general, a record of decision is adequate if someone who's not familiar with the decision could be reasonably informed about the decision.

Carefully consider what is required to adequately document a decision. In some cases, an adequate record of a decision may be a brief note in a case management system or a case file; in other cases, it may be made up of numerous extensive studies.

Ensure you're storing records of decisions and the records you create in the most appropriate place in your office's recordkeeping system. Office recordkeeping systems do not include locations that are only available to you, such as your email account or desktop.

The BCER does not have to create and keep records of every decision made by every employee. BCER staff need to identify which decisions are to be documented by applying your judgement in the context of our specific mandates and with consideration to the purpose and intent of the IMA, [the directive and the guidelines](#), and other obligations that may exist in law and policy respecting documenting decisions.

#### Why document decisions?

- Supports openness and transparency
- Facilitates effective decision making
- Preserves corporate memory
- Supports employees in doing their jobs effectively and providing high quality services to the public
- Supports accurate reporting of decisions to stakeholders, including other government bodies and the public
- Contributes to the Province's historical record for future generations

### Records: Documenting decisions

Which of the following statements are true for government bodies?  
**Select all that apply.**

- Must use appropriate systems for maintaining adequate records of decisions
- Should ensure that key decisions are securely maintained on personal drives
- Does not have to create and keep records of every decision made by every employee
- Needs to identify which decisions are to be recorded by considering context, the purpose and intent of the IMA, CRO directives and guidelines.



[DOWNLOAD DOCUMENTING GOVERNMENT DECISIONS ACTIVITY DESCRIPTION](#)

[See here](#) to learn more about the Documenting Government Decisions CRO Directive and Guidelines.

[See here](#) for Regulator Documenting Decisions guidance.

## Shared responsibility

BCER staff are responsible for documenting their work by ensuring records they create or receive are adequate, and are filed in their office recordkeeping system, including email.

Program areas are responsible for maintaining a shared office recordkeeping system that's organized and administered in accordance with information management legislation and policy.

Your office recordkeeping system does not include locations that are only available to you, such as your email account, computer hard drive, OneDrive or desktop.

And remember, the directive and guidelines for Documenting Decisions specifically define the requirements for creating and maintaining government information that is an adequate record of a government body's decisions.

**Common types of recordkeeping systems include:**

A Shared Drive structure with ARCS and ORCS applied; line of business applications, organized and governed SharePoint sites, and physical filing systems (e.g. paper in the FSJ Records Centre).

### Scenario – cleaning up email before going on vacation

Drew is going on vacation for three weeks and has been working on several time-sensitive projects and keeping their work in personal drives and email. Feeling overwhelmed, Drew reaches out to Maria, who has excellent records management habits.

What advice would Drew get from Maria?

**Select the best option.**

- Option A)** To leave the records as they are or send anything important to Maria as an email attachment just in case.
- Option B)** To review their project email and files, to delete duplicate information and to identify final email and email chains that contain the complete record and to save them in the team's shared project file, including any substantive notes and drafts or final documents.

SUBMIT

[DOWNLOAD CLEANING UP YOUR EMAIL BEFORE GOING ON VACATION ACTIVITY DESCRIPTION](#)

## Information schedules

Information schedules are our primary tools to manage government information effectively over time. They:

- Describe and classify government information
- Set out the final disposition of a record (that is, whether it will ultimately be transferred, archived or destroyed)

- Are approved under the IMA
- Increase efficiency
- Uphold the trust that comes with the obligation to protect government information

Understanding schedules is critical to help your organization meet its obligations under the IMA. In the BCER, we use ARCS, ORCS (the Oil and Gas Regulation Operational Records Classification System), and Special Schedules, such as the Transitory and Executive Records Schedules.

Click on the three main types of schedules below to see why each is important to your work.

[ARCS](#)

[ORCS](#)

[Special Schedules](#)

## Transitory information

Transitory information is information of temporary usefulness that's needed only for a limited time to complete a routine action or prepare a final record. It can exist in any format or medium (paper or digital) and can be created and shared using a variety of technologies (e.g., email, social media, Teams, SharePoint).

By promptly removing transitory information (also known as transitory records), employees are better able to identify and file key records into their recordkeeping system, where they can be easily found. As well, the BCER avoids unnecessary costs for storing and processing transitory records. Transitory records are covered by the Special Schedule for Transitory Records (schedule 102901). They do not need to be filed using ARCS or ORCS.

Who can apply the Transitory Records schedule? You! The authority to identify transitory records is delegated to each B.C. public servant. Transitory information can and should be disposed of when it's no longer of value, with one important exception: if the Regulator receives an FOI or litigation search request, all relevant records must be provided, including transitory information that exists at the time of the request. Transitory information that's subject to such requests must be retained pending completion of the applicable FOI response process and review period or the applicable litigation activities.

Use this [Transitory Records Guidance](#) to determine whether the information is transitory.

A record's content and context determine whether it is transitory, not its format or storage medium. If an email, draft document, or other record is essential to understanding the Regulator's business – e.g. how a particular decision was reached – then the record is not transitory and must be kept.



### Which of these statements are true?

Select all that apply.

All instant messages are transitory

Transitory information can be destroyed when no longer needed, unless it is relevant to a search for legal purposes, or an active FOI request

Deleting information makes it transitory

Records containing transitory information are subject to FOI

Submit

DOWNLOAD TRANSISTORY INFORMATION ACTIVITY DESCRIPTION

## Creating and managing email

All employees are encouraged to follow email management best practices, as set out in the [email guidance on the Energy Exchange](#). This material provides detailed information on using your email account, including sending, searching and managing email, and protecting sensitive information. If you apply these and other best practices, it will make it easier to find the information you need, while also ensuring that information is available to your colleagues when you are not in the office, and in the event of an FOI request or litigation search.

## Creating and Managing Email

DO	DON'T
Regularly file email that is material to business operations and decisions in the office recordkeeping system	File transitory emails
Use separate email threads for different subjects	Create unnecessary email and email attachments
Use meaningful and concise subject lines	Use your personal email accounts for BCER business
Regularly dispose of transitory email and utilize Outlook tools and features to help (e.g., the "clean up conversation" tool)	Rely solely on email and similar technologies when making important decisions, and if you do use email, ensure that the email adequately documents a decision and make sure to file it
Keep personal use of your BCER email account to a minimum	Triple delete emails







[DOWNLOAD CREATING AND MANAGING EMAILS ACTIVITY DESCRIPTION](#)

It's important to remember, when you file email into your recordkeeping system, the original email in Outlook is redundant and should be deleted. Not doing so may cause confusion as to which copy is the official record.

## Do I need to keep every email? When can I delete an email?

You need to save all emails that pertain to the business of the Regulator, except for transitory emails. You may delete transitory emails when they're no longer needed. You must not delete any emails that may be responsive to an active FOI request or request for legal discovery. You should save emails that document an important government decision.

Consider the implications of these two different approaches to managing email. Click each scenario to see how these practices could impact your work or the work of others.

<b>Scenario 1</b>	<b>Scenario 2</b>
Keeps every email 'just in case' they may need it 	Deletes transitory email when no longer needed 
Relies on their email folders for keeping records of important decisions 	Routinely files important email, including evidence of project decisions, on the shared project folder 
Always shares information and collaborates on drafting through email attachments 	Collaborates on drafting documents housed in the shared project folder 


# Disposal of BCER information

We've already established that information schedules govern how long records are needed and when they may be appropriately archived, disposed of or transferred to another organization. The BCER Records and Information Services Branch manages the disposal of information through the transfer of records to the government archives, or following our [Documented Destruction Process](#).

### How do we Dispose of Information

Disposal of government information must be carried out in a **secure** and **confidential** manner.

The more **sensitive** the information is, the more measures we should take to ensure that it is **securely** and **appropriately destroyed**.



## Resources

BCER's Records and Information Services (RIS) is committed to providing services, resources and learning tools that support you and the BCER. Our [Energy Exchange](#) pages contain guidance on everything we covered in this section and more.

RIS is here to help you with the following services:

- Records management advice for all types of records
- Online guides and eLearning
- Information schedule advice
- Shared Drive Organization and Collaborative Digital Workplace (SharePoint) projects
- Accessing physical records

We encourage you to contact [RecordsManagement@bc-er.ca](mailto:RecordsManagement@bc-er.ca) for assistance.

CLOSE THIS TAB



The Freedom of Information and Protection of Privacy Act (FOIPPA) outlines the circumstances in which public bodies, such as BCER, can collect, use and disclose personal information. FOIPPA requires that all public servants protect the personal information that we hold. Privacy is a complex topic. This course supports BCER employees with an understanding of how to handle personal information responsibly and lawfully.

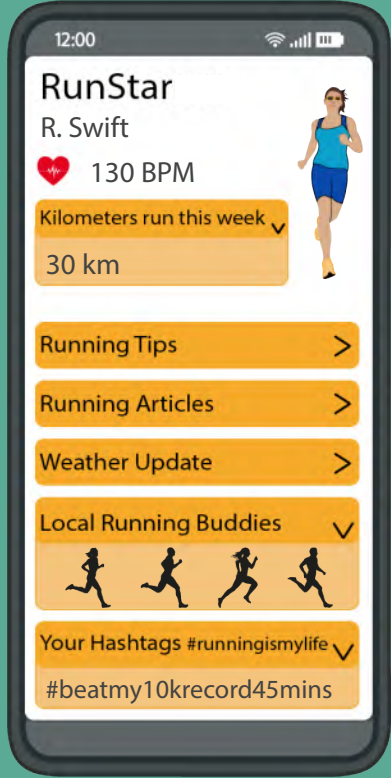
## What is personal information?



Personal information is recorded information about an identifiable individual other than their business contact information. Personal information can include things like someone’s name, home address and home email. It also includes their educational history, employment history, and even their personal opinions.

Some types of personal information can be considered sensitive because there is a higher risk of harm to individuals if the information is improperly collected, used or disclosed. Sensitive personal information is not defined in FOIPPA. Some examples of what may be considered sensitive personal information include: DNA, personal health history, information about sexual orientation, gender identity, religious or political beliefs, and race or ethnicity.

All personal information must be treated as confidential information.



**Personal information –  
The RunStar running app**

A ministry co-worker is working on a fitness app that the ministry plans to make available to support healthy habits.

Click on data elements in the app that may be treated as personal information when provided together in this running app.

[Click here to reveal answers](#)

## Business contact information

Personal information does not include business contact information – information that enables you to contact someone for work purposes – such as a name, work phone number or email address. Yet, some contact information can be considered personal if it's being used for personal reasons.



**BCER**  
BRITISH COLUMBIA ENERGY REGULATOR

[www.bc-er.ca](http://www.bc-er.ca)

**BCER Staff member**  
Manages Information  
Protector of Privacy

**Excellent Services Division**  
BCER.SuperStar@bc-er.ca

**T. 250-419-1234**  
**F. 250-419-4403**  
**M. 123-456-7890**  
24-Hour 250-794-5200

2950 Jutland Rd.  
Victoria, BC V8T 5K2

Click the buttons below to review the Scenarios



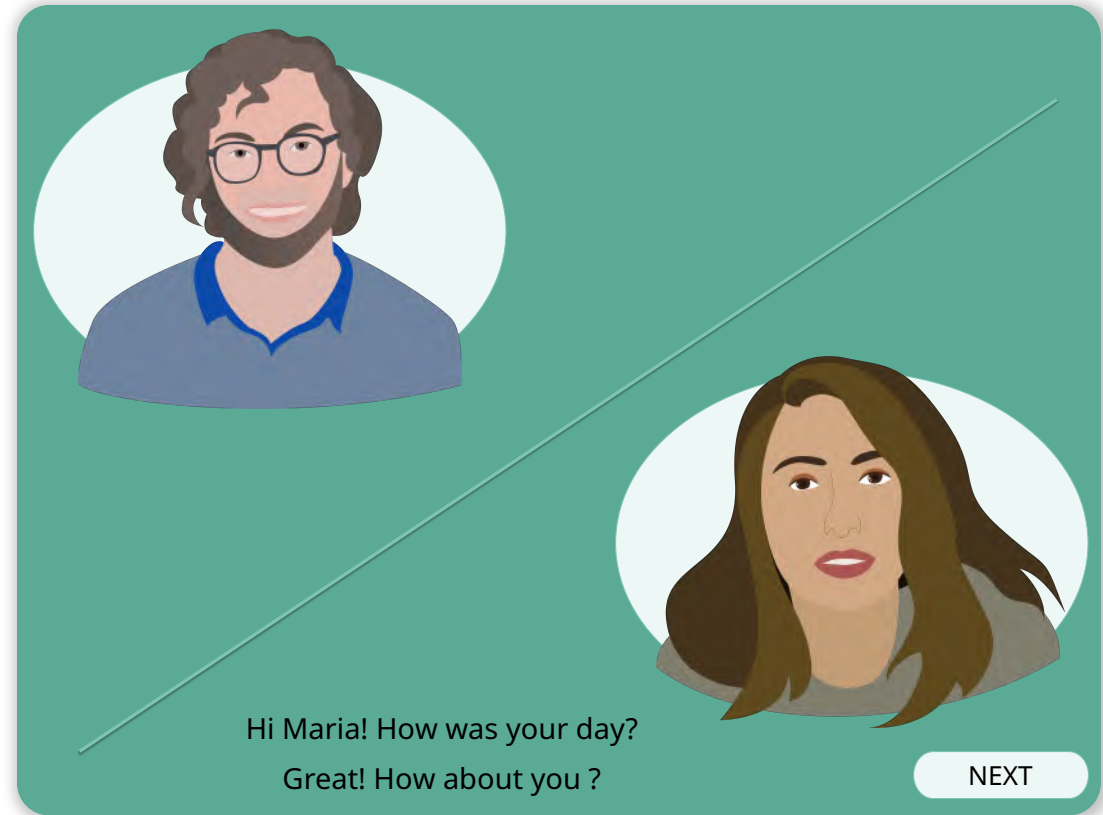


## The mosaic effect

The mosaic effect occurs when information that appears to be non-identifiable is combined in a way that can reveal the identity of an individual. For example, an email address may not contain an individual's name but when you can see information that email address is associated with (e.g., website user accounts set up by that email), you might be able to identify the email address's owner. If you can combine information about an individual's hobbies and hometown you may not be able to identify anyone if they are an avid foodie from Vancouver but an elite trampolinist from Oliver, B.C. might be more easily identified.

Think about the mosaic effect when seeking to understand privacy implications. While medical records, dates of birth and home addresses are easily recognizable as personal information, individuals can often be identified within data that has been de-identified.

Consider the mosaic effect in this conversation about a hiring competition that Drew is managing.



DOWNLOAD MOSAIC EFFECT IN A CONVERSATION ACTIVITY DESCRIPTION

## Freedom of Information and Protection of Privacy Act

As employees of a public body bound by FOIPPA, we are all responsible for ensuring that our work is carried out in accordance with B.C.'s privacy legislation.

You may have access to personal information that your program area has collected for an authorized purpose. B.C. public servants can only access, use or disclose personal information where required and authorized to do so for work; we cannot do so for our own purposes. Accessing information without the

appropriate authority may result in an information incident that would need to be reported.

FOIPPA also requires that public bodies protect personal information. The BCER does this by using reasonable security controls, ensuring that individuals who handle personal information are aware of their responsibilities, and completing privacy impact assessments.

## Privacy principles at work

As B.C. public servants, we need to handle personal information appropriately. When you access personal or other confidential information, consider how your plans for the information align with privacy principles.

You can find out more about privacy principles here: [Ten Privacy Principles](#)

### Privacy principle: Identify purpose

Select the questions that you should ask yourself that are related to the above principle.

- Why do you need the personal information?
- Is all of it needed for the task at hand?
- Did you get this personal information from an appropriate source?
- What are you doing to protect the information while you access it?
- Are you using information for a legitimate purpose?
- Before you share information, how do you know it's okay to share it?

## Privacy impact assessments

Privacy impact assessments (PIAs) are tools to evaluate the privacy implications of new and existing enactments, systems, projects, programs or activities. PIAs must be started early in the development process for new initiatives that the BCER introduces and any changes that are to be implemented. Complete PIAs before the program is launched and always before any personal information is collected, used or disclosed.

PIAs promote transparency, accountability, and contribute to continued public confidence in the way the government manages personal information.

### Starting a new project

Maria is helping to design a new program to provide services for residents. How can they ensure privacy is considered appropriately in this new program? Select all that apply and click SUBMIT:

- Start collecting the personal information that's available. Information that's not necessary can be deleted later
- Reach out to the Privacy Officer
- Draft a PIA, even if there are still details to be worked out
- Email the PrivacyOfficer@bc-er.ca to be granted your FOIPPA authorities

SUBMIT

[DOWNLOAD STARTING A NEW PROJECT ACTIVITY DESCRIPTION](#)

Maria was processing an application for someone who had applied for services. He seemed nice and Maria thought he'd make a good candidate for a focus group her team was putting together on a different topic. Maria asks Drew the following question.

Hey, I was thinking about reaching out to one of your clients to see if he'd like to participate in a focus group on a new potential service I'm working on. His personal information would have been included in his application to your program. Do you think it's alright if I add him to the list of participants to be contacted?



NEXT

[DOWNLOAD PROCESSING AN APPLICATION ACTIVITY DESCRIPTION](#)

## Information incidents

An information incident is a single or a series of events involving the collection, storage, access, use, disclosure or disposal of government information that threaten privacy or information security and or contravene law or policy. Information incidents can involve confidential or personal information. A privacy breach is a type of information incident.

## Reporting information incidents

If you discover or suspect an information incident, report it immediately by calling the BCER Privacy Officer, or email [PrivacyOfficer@bc-er.ca](mailto:PrivacyOfficer@bc-er.ca).

## Notify your supervisor

Keep your supervisor informed of the incident. They can support you as you work with an investigator to respond to the incident.

## Next steps

Once an information incident has been reported, the Privacy Officer will contact you to assess the incident and provide recommendations on the steps to take.

The investigator will work with you to:

- Report to the appropriate stakeholders
- Contain the incident and recover any information that was inappropriately disclosed
- Remediate including determining whether notifying impacted parties is necessary
- Create strategies to prevent a future incident (for example, privacy training).



### Considerate Carlos

Carlos volunteers for a community association and he thinks one of his clients might be interested in joining. He decides to look him up in the system he has access to at work to find out more. Is this allowed?

- Yes, it sounds like he's trying to be helpful.
- No, this is not allowed.

SUBMIT

[DOWNLOAD CONSIDERATE CARLOS ACTIVITY DESCRIPTION](#)

### Information Sharing Agreements

Public bodies enter Information Sharing Agreements (ISAs) when there's a regular and systematic exchange of personal information between public sector organizations or between a public sector organization and an external agency. ISAs document the terms and conditions of the exchange of personal information in compliance with the provisions of the Act and any other applicable legislation. Contact RIS if you are considering entering into or initiating an ISA.

## Privacy resources

There are [privacy resources](#) on the Energy Exchange, which will help you make informed decisions about handling personal information.

We encourage you to contact [PrivacyOfficer@bc-er.ca](mailto:PrivacyOfficer@bc-er.ca) if you have any questions.

CLOSE THIS TAB



# Access to Information

Rain Forest, Abbotsford

## Freedom of Information requests

In this section, we'll discuss access to information, and talk about both Freedom of Information — or “FOI” — and proactive disclosures of information outside of the FOI process.

The [Freedom of Information and Protection of Privacy Act](#) (FOIPPA) provides individuals a right to access their own personal information held by public bodies, as well as general information about government operations, programs and services – with limited exceptions.

The BCER is committed to expanding the public availability of government information and data through the disclosure of information without a formal FOI request. Whenever possible, information is released to the public as permitted or required by law.

Anyone can make an FOI request. We have a responsibility to be open, transparent and to provide people with the records to which they have a right of access. We receive FOI requests from a wide variety of applicants, such as: industry, individuals, political parties, the media, law firms, businesses, researchers, interest groups and other governments.

A person can ask for any record through FOI, but the request needs to be clear enough for an employee to identify the record. For the purpose of FOI, a record includes anything on which information is recorded or stored.

Access to information in a record is granted based on a line-by-line review, to ensure that the information is legally appropriate for release to the applicant that has asked for it, as permitted or required by law.

BCER employees have a “duty to assist” an applicant by taking all reasonable steps to respond quickly and accurately.

#### **Duty to Assist:**

Employees have a responsibility to be open and to connect people with the records to which they have a right of access, even if the request wasn't necessarily worded clearly. You must look to fulfill the underlying intent of the request.

## **Records & Information Services (RIS) and you: a partnership**

RIS is the centralized point of contact for processing BCER FOI requests. FOIPPA specialists administer the day-to-day work of providing timely responses to FOI requests received by the Regulator. The FOI team works with program areas to search and gather records. RIS works closely with you, because you are the subject matter expert on the records you work with. You know what information you hold, and whether the information is responsive to a FOI request.

You are in the best position to identify whether something may be harmful if it were released — you're not expected to know what section of FOIPPA may apply in terms of removing information. But you should let RIS know if you have additional information that may be relevant to the decision about whether information should be severed.

#### **Severing Information:**



There are reasons the Regulator will remove – or ‘sever’ – information from a record prior to releasing it to an applicant.

Ultimately, disclosure recommendations are made by the RIS FOIPPA Specialist and based, in part, on the context you provide regarding possible harms to government or third parties. A final decision with respect to disclosure, relying on RIS’s recommendations and supported by your input, is made by the delegated head for the BCER.

The FOI team at the BCER are the experts when it comes to processing FOI requests. They have the expertise required to apply FOIPPA, to manage the legislated timelines, and to communicate with the applicant that made the FOI request. RIS also possesses the technology required to effectively sever information from records as required or permitted by FOIPPA.

### FOI requests: roles and responsibilities

Take a moment to review this high-level overview of the FOI process for BCER. Remember that the purpose of this process is to create a system that will ensure an effective, customer-focused experience.

BCER Staff

BCER FOIPPA Specialist

As a member of public service you are:

Click to reveal the bullet points



- 1 The subject matter experts on the records you use, what information your branch has, and whether the information you and your program area have is responsive to a FOI request
- 2 In the best position to work with RIS to properly interpret or clarify what an applicant is looking for
- 3 Not expected to know what section of FOIPPA may apply in terms of removing information
- 4 In the best position to identify whether something may be harmful if it were released
- 5 Responsible for ensuring this information is communicated back to RIS


It's important to note that FOIPPA includes timelines for responding to FOI requests.

## The five stages of an FOI request

### The five stages of a FOI request

The graphic below illustrates the five steps FOI requests may go through. Click the steps to review

- Intake**  
RIS assists applicants in refining their FOI requests so that the requests meet legislated requirements and are as clearly defined and specific as possible.
- Search**  
RIS works with program areas to conduct a records search, complete a harms assessment, and provide information necessary to support fee estimation.
- Review**  
RIS conducts consultations, takes time extensions where required and permitted, and reviews and analyzes information to make disclosure recommendations.
- Approve**  
RIS facilitates the approval of the disclosure recommendations.
- Release**  
RIS releases the records package to the applicant and publishes to the BCER website, where applicable.

 Scroll down to continue the module

## Want to learn even more about the FOI process?

### These links are recommended:

- [FOI in the BCER](#)
- [BCER Internal FOI Process Flowchart](#)
- [FOIPPA Policy & Procedures Manual](#)
- [BCER – Freedom of Information](#)

## How to fulfill your duty to assist

BCER employees must make every reasonable effort to assist FOI applicants, and to respond to every FOI request openly, accurately, completely and without delay. After all, access to information is a foundational democratic principle.

The “duty to assist” goes beyond just meeting the letter of the law — it involves providing an excellent service experience to each applicant.

To meet your duty to assist an FOI applicant, you need to interpret FOI requests in the best interest of the applicant. This means steering clear of overly narrow interpretations, requesting clarification of requests when necessary and ensuring you’re being diligent in your search for responsive records.

To fulfill your duty to assist:

- Adequately interpret FOI requests as a fair and rational person would expect – and in good faith
- Make a solid effort to discern the intent and goal of the requestor
- Conduct thorough searches for records (e.g. Outlook, Shared Drives, Teams, OneDrive, electronic systems, databases and any other office recordkeeping system) and document the search effort

## FOI: The search process

A diligent search for records is one of the most important things you can do to assist people in accessing the information that they want. You are responsible for searching anywhere you have reason to believe recorded information might be stored that could be relevant to the request.

The BCER needs to provide evidence that a thorough and comprehensive search has been conducted. That’s why it’s very important that you document the details of your efforts, as well as an explanation in the event of a no-records response. Following good records management practices within your email and recordkeeping systems makes searching for records and responding to FOI requests much easier.

The search process must be thorough and widespread enough to ensure that all responsive records are located.






As we've already learned, emails are only one type of government records, and an adequate search for records that could be responsive to an FOI request requires more than just searching emails.


When conducting a search, you need to look in your office's electronic recordkeeping systems on Shared Drives, SharePoint sites and other collaboration tools, and in your paper or electronic notebook, as well any paper files.

The FOIPPA Specialist is your point of contact and will provide support to you to ensure you have a clear understanding of the request and what is required of you in responding.

### Conducting a thorough search for records

Maria is doing a records search. A thorough search would include which of these places? Click on all the places she should search then click SUBMIT

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Microsoft Teams	File folders	Post-its	Cell phone	Email
				





To conduct a thorough email search:

- Search all Outlook items, not just your Inbox
- Search every mailbox you have access to, not just your own mailbox
- Search deleted, sent and subfolders
- Use broad search terms
- Use your expertise and knowledge on the topic to find everything that may be relevant
- Search common acronyms and synonyms

Also search for individual emails you may have printed or filed elsewhere.

If you have .PST files or have preserved emails in .PDF format to the hard drive of your computer or a Shared Drive, search these files if you have reason to believe relevant records may be saved there.

#### **A note about archived emails:**

If you have archived email files saved in a recordkeeping system, you may need to search those files as well. This is important to remember, because a search through your email account will not capture these files, which could contain records responsive to a request. This also applies to individual emails you may have saved elsewhere, outside of your email application.

## **PST files**

PST files contain batches of Outlook content including emails, calendar events, tasks, etc. Folders, inboxes or entire mailboxes can be exported from Outlook in this format. PST files are not recommended for preservation purposes because they handle poorly in LANs, are easily corruptible, can't be searched in EDRMS environments, and can't be scanned for viruses. Contact the IT department at [servicedesk@bc-er.ca](mailto:servicedesk@bc-er.ca) for assistance with searching PST files.

## **Summary**

It is also important to remember, that even transitory records need to be included if you have not yet disposed of them when the FOI request is received. You are not permitted to dispose of transitory records if they're responsive to an ongoing FOI request.

## Proactive disclosure

Proactive disclosure is the disclosure of information without the need for an FOI request. The BCER has a robust system that supports the proactive disclosure of information and discloses many kinds of data and information outside of the FOI process. Information is routinely released by responding to requests for information informally, as often as possible. In addition, the [BCER website](#) contains technical, spatial, analytical and other types of data and reports which are updated regularly, and available to the public.

The B.C. Data Catalogue also provides the easiest access to government's public data holdings, as well as applications and web services. Thousands of the datasets discoverable in the catalogue are available under the Open Government License — British Columbia.

We encourage you to contact [FOIIntake@bc-er.ca](mailto:FOIIntake@bc-er.ca) if you have any questions.

CLOSE THIS TAB

# FOIPPA Foundations

## Privacy and Access Fundamentals



## Overview

British Columbia's [Freedom of Information and Protection of Privacy Act](#) (FOIPPA) requires that public bodies, such as ministries, municipalities, and universities—along with public body contractors and service providers—protect all personal information they hold.

**It's an important job!**

### Your responsibilities

As a public body employee, or service provider to a public body, you are required to protect personal information you handle in the course of your work. At the same time, you must make every reasonable effort to assist members of the public in their requests for information.

This course introduces the key ideas behind the Freedom of Information and Protection of Privacy Act (FOIPPA). By the end of it, you will be able to:

- Describe fundamentals of FOIPPA
- Describe your responsibilities under FOIPPA
- Describe how FOIPPA applies to your work
- Identify your privacy and access obligations

## This course

The intended audience for this course is primarily B.C. public body employees and service providers to B.C. government. This course should take you about 60 to 90 minutes to complete. It consists of three modules:

Module 1: **The Basics** ^

Module 2: **Protection of Privacy** ^

Module 3: **Access to Information** ^

Each module also includes a Tip Sheet you can download to help you access and remember key information.

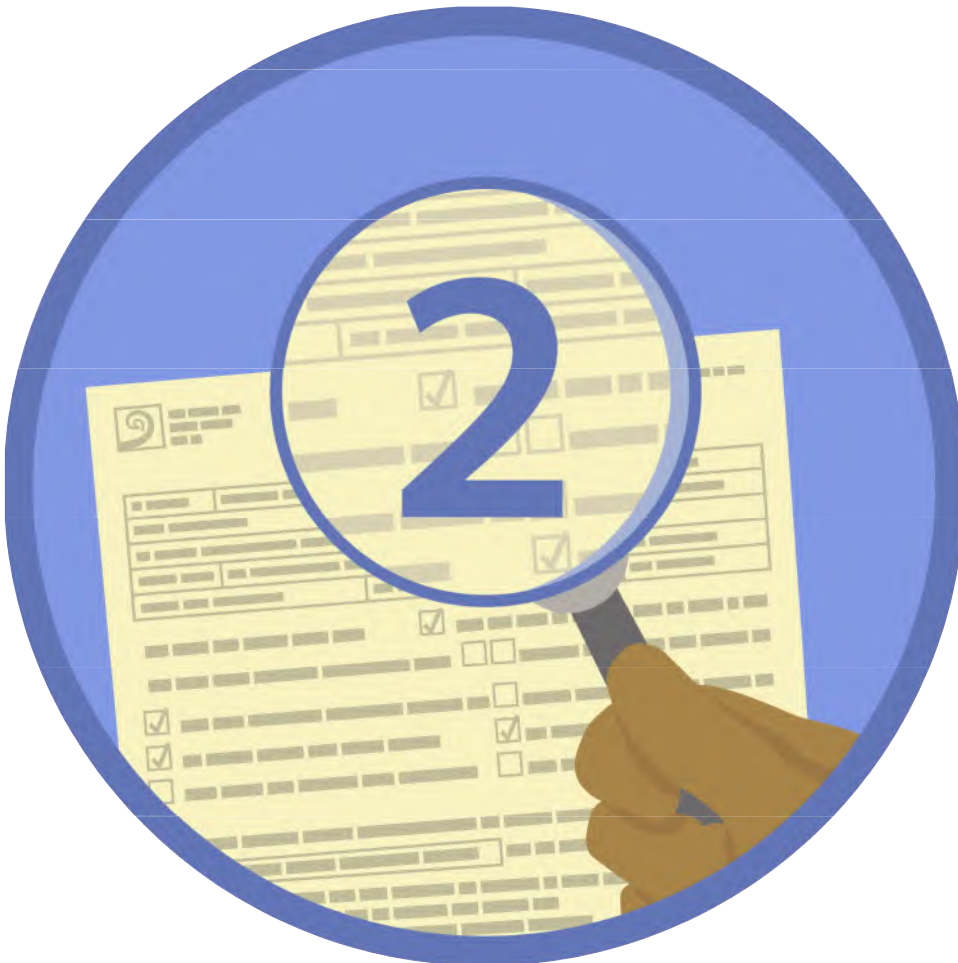
## The exam

This course ends with a 10-question, multiple-choice exam to test your knowledge of key concepts from the course.

You will need to answer 80% of the questions correctly to pass. You may take the exam as many times as you like. As soon as you have passed the exam, you will be able to download a certificate of course completion.

# Modules

Select a module below to get started:





We acknowledge all Indigenous peoples on whose territories we live, work, and play. We honour their connection to the land and respect the importance of the diverse teachings, traditions, and practices within these territories.



Ministry of  
Citizens' Services



# Module 1: The Basics

# TIP SHEET



The Freedom of Information and Protection of Privacy Act (FOIPPA) is the privacy and access legislation that governs all public bodies in B.C. As a public body employee, contractor, or service provider, you must ensure that you manage information in accordance with FOIPPA.

## Four domains of information management

Records management, access to information, privacy, and security all play an important role in the effective stewardship of information held by public bodies.

- 1** **Records management:** Records management is the system an organization uses to effectively capture and maintain information associated with business activities and transactions. Records include both print and digital records of such items as email, documents, maps, and handwritten notes.
- 2** **Access:** Public bodies are accountable to the public for ensuring access to records under the custody or control of the public body, with limited exceptions. This includes individuals' right of access to their personal information.
- 3** **Privacy:** Privacy is protected by public bodies treating personal information responsibly and lawfully. This includes ensuring personal information is collected, used, and disclosed appropriately.
- 4** **Security:** Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability of that information or system.



# Module 1: The Basics

# TIP SHEET



## Where to go for help

- **Your supervisor** can help you determine when and how you are authorized to collect, use, and disclose personal information in the course of your work.
- **Your privacy officer** is the point of contact for privacy in your organization and can help you understand and resolve privacy issues, as well as navigate such processes as completing Privacy Impact Assessments.
- **Your FOI coordinator** is an expert in access to information and can help you navigate responding to FOI (access) requests.
- **The corporate privacy office** within the Ministry of Citizens' Services provides services to government and the broader public sector, including privacy training and resources such as the Privacy & Access Helpline.
- **The Office of the Information and Privacy Commissioner (OIPC)** provides independent oversight and enforcement of B.C.'s access and privacy laws, including the Freedom of Information and Protection of Privacy Act (FOIPPA). The office also has resources on privacy and access for public bodies, organizations, and individuals.

## Custody and control

FOIPPA applies to all records in the custody or under the control of a public body, unless explicitly out of scope of the Act.

- **Custody** of a record means physically possessing that record. It normally includes responsibility for, access to, and security of, that record, as well as managing, maintaining, preserving, and disposing of it.
- **Control** of a record refers to the authority to make decisions about how a record ought to be managed throughout its lifecycle. If a public body has control of a record, even if it does not have custody of that record, the record still may be subject to FOIPPA. For example, a public body's records that rest with one of its service providers would be under its control but may not be in its custody.





# Module 2: Protection of Privacy TIP SHEET



The Freedom of Information and Protection of Privacy Act (FOIPPA) works to protect personal privacy by preventing the unauthorized collection, use, or disclosure of personal information by public bodies.

## Personal information

Personal information is recorded information about an identifiable individual other than their business contact information. It includes information about an individual's education history, employment history, health history, and even their personal opinions. It may also, depending on the circumstances, include other information, such as the person's name, home address, and DNA.

## Questions to consider when handling personal information:

1. Why do I need the personal information?
2. Am I authorized to collect the information at this particular time (for example, is all of it directly related to and needed for the task at hand)?
3. What am I doing to protect the information I handle?
4. Am I using the information for a purpose consistent with why it was collected? If not, have I obtained **consent**?
5. Am I authorized to share the personal information?

## Authorities

If a public body wants to collect, use, or disclose personal information, it needs to have an authority under FOIPPA to do so. These authorities outline the specific circumstances in which public bodies can **collect, use, and disclose** personal information.

As a public body employee or service provider to a public body, you may only access personal information that your public body has **collected in circumstances where it is required for your work and authorized under FOIPPA**. You may not access it for your own purposes.



# Module 2: Protection of Privacy

## TIP SHEET



### Privacy tools

Privacy impact assessment (PIA)	Helps identify possible impacts to individuals' privacy from new and existing initiatives
Information sharing agreements (ISAs)	Documents the terms and conditions of the exchange of personal information in compliance with legislation
Information Sharing Code of Practice	Supports responsible and lawful personal information sharing and the protection of personal information
Privacy schedule in contracts for service providers	Ensures service providers maintain the privacy standards for personal information set by FOIPPA

### Disclosing and storing sensitive personal information outside of Canada

A public body must complete a supplementary assessment for disclosures outside Canada when a program, project, or system includes *sensitive* personal information that is *stored* outside Canada. For more information, see [Guidance on Disclosures Outside of Canada](#).

### Information incidents/privacy breaches

An **information incident** is an event (or series of events) involving the collection, storage, access, use, disclosure, or disposal of confidential or personal information that threatens privacy or information security, and/or contravenes law or policy.

An information incident that threatens privacy is called a privacy breach and includes the theft or loss of personal information, or the collection, use, or disclosure of personal information that is not authorized by FOIPPA. A privacy breach may be accidental or deliberate.

There is a privacy breach notification requirement in FOIPPA. If there is a reasonable risk of significant harm to an individual as a result of a breach, the head of the public body must notify the affected individual and the Office of the Information and Privacy Commissioner (OIPC). Notification allows the individual affected by a privacy breach to take steps to mitigate possible harm.



# Module 2: Protection of Privacy

# TIP SHEET



## Responding to an information incident/privacy breach

If you suspect an information incident/privacy breach has occurred, your first step is to immediately report the incident to the appropriate contact.

- **Public body employees** report to your supervisor, privacy officer, or other designated contact in your organization.
- **B.C. government employees, contractors or service providers** call 250 387-7000 or toll-free at 1-866-660-0811 (select option 3).

Once reported to the appropriate contact in your organization, they will help you through the remaining **steps to respond to the incident**.

In situations where containment of the information is possible (such as requesting an unintended recipient double-delete an email), consider making this request as soon as possible and advise the appropriate contact of steps taken.

# Module 3: Access to Information TIP SHEET



Under the **Freedom of Information and Protection of Privacy Act (FOIPPA)**, individuals have a right to access:

- Their own personal information held by public bodies
- General information held by public bodies, including information about government operations, programs and services, with limited exceptions

**Access to information is:**

- A foundational democratic principle, supported by FOIPPA
- Permitted or required by law
- Granted based on a line-by-line review of the record to ensure that the information is legally appropriate for release to the person requesting it

Anyone, including individuals, political parties, media, law firms, businesses, researchers, interest groups, or other governments, may make an FOI request. An applicant may submit a request to access a record in any written format. If the applicant is making the request on behalf of another person, the applicant must also provide written permission from the other person (unless permitted by the **FOIPP Regulation**).

## FOI exceptions to disclosure

While the public body’s intention should always be to release information wherever possible, FOIPPA lists a number of **exceptions** to the release of information. These exceptions provide public bodies with the authority to sever (take out) information from a record before releasing it. The person who made the request retains the right to access the remainder of the record.

Mandatory exceptions	Discretionary exceptions
<p>Public bodies <b>must</b> withhold information:</p> <ul style="list-style-type: none"> <li>• Subject to cabinet confidences</li> <li>• Harmful to the interests of an Indigenous people</li> <li>• Harmful to the business interests of a third party</li> <li>• Harmful to a third party’s personal privacy</li> </ul>	<p>Public bodies <b>may</b> withhold information that is:</p> <ul style="list-style-type: none"> <li>• Subject to local public body confidences</li> <li>• Policy advice or recommendations</li> <li>• Legal advice</li> <li>• Harmful to: law enforcement; intergovernmental relations or negotiations; financial or economic interests of a public body; conservation of heritage sites; or, individual or public safety</li> </ul>



# Module 3: Access to Information TIP SHEET



In general, once a public body receives a request, the public body:

1. **Reviews the request** to clarify and/or determine if the information being requested is already available to the public
2. **Confirms receipt of the request.**
3. **Assigns a file number or method** of tracking the request.
4. **Establishes fees** to charge for the request (if any). Public bodies must not use fees to discourage an applicant from proceeding with a request.
5. **Searches for the record** anywhere there is reason to believe recorded information relevant to the request might be stored—and document the details of the search.
6. **Retrieves the record.**
7. Completes a **line-by-line review** of the information to determine what information (if any) may or must be severed before release. See [FOI Exceptions to Disclosure](#).

If some information must be severed, the public body must give the reasons, in writing, for refusing access to that information, as well as:

- The FOIPPA provision(s) on which the refusal is based
  - Contact information for an employee who can answer the applicant's questions
  - Information about how to ask the Office of the Information and Privacy Commissioner to review the decision.
8. **Provides results to the applicant** within a maximum of 30 business days from the time the request was received.

**Third parties:** A public body may receive a request for access to a record that, although in the public body's custody, was either not authored by the public body or relates to a third party. If the public body thinks there may be harm in giving access to that information, it should consider whether they may or must consult with the third party before making a decision ([s. 23/24](#)).

**Extensions:** FOIPPA permits public bodies to take a 30-day extension for a number of reasons ([s. 10](#)). The Office of the Information and Privacy Commissioner (OIPC) may also authorize a public body to take an extension for periods longer than 30 days for the same reasons, or if the OIPC otherwise considers that it is fair and reasonable to do so.

**Proactive disclosure:** Public bodies are required to establish categories of records that are in their custody or control that are available to the public without an FOI request ([s. 70](#) and [71](#)) and to immediately disclose information where it relates to a risk of significant harm to people or the environment, or where disclosure is clearly in the public interest ([s. 25](#)).



# Overview of the BCER's FOI Process

Information for the BCER's Internal FOI Review Group/Leadership

Prepared by:  
Records & Information Services Branch – FOI Team

*Updated: April 2023*

# FOI Request Processing – Typically 30 Business Days to...

1. Respond to an applicant (acknowledge/clarify request)
2. Notify appropriate staff/departments of new request
3. Search for/gather all responsive records
4. Combine and collate records into PDF format
5. Review records for responsiveness (relevance to request)
6. Review records for “harms” (line-by-line review) and withhold under appropriate sections of FOIPPA (“severing”; “redlining”; “redacting”)
7. Circulate draft release package for review by Leadership/SMEs – to identify missed harms and/or information that can safely be released
8. Circulate draft release package for review by Public Trust (Executive Director) and Legal Services for issues management/legal perspective
9. Complete any required edits (finalize the release package)
10. Obtain final sign-off by Delegated head
11. Release to applicant



# FOIPPA's Exceptions to Disclosure...

The *Freedom of Information & Protection of Privacy Act* (FOIPPA) has **mandatory** and discretionary exceptions to disclosure:

- **S.12** – Cabinet confidences
- S.13 – Policy advice or recommendations
- S.14 – Legal advice
- S.15 – Disclosure harmful to law enforcement
- S.16 – Disclosure harmful to intergovernmental relations or negotiations
- S.17 – Disclosure harmful to financial or economic interests of a public body
- S.18 – Disclosure harmful to the conservation of heritage sites, etc.
- **S.18.1** – Disclosure harmful to interests of an Indigenous people
- S.19 – Disclosure harmful to individual or public safety
- S.20 – Information that will be published or released within 60 days
- **S.21** – Disclosure harmful to business interests of a third party
- **S.22** – Disclosure harmful to personal privacy

# Current FOI Process

1. Formal written request is received from applicant (and logged)
2. Email notification of request/“call for records” is sent to program staff (those thought to hold records)
3. Responsive records are gathered by staff (or, in some cases, directly by FOI) and forwarded to Internal FOI for processing
4. Received records are collated/combined into single PDF
5. Records are reviewed by Internal FOI for responsiveness and “harms”; severing is applied pursuant to FOIPPA’s exceptions to disclosure
6. Draft release package is circulated to internal FOI Review Group for feedback and VP approval ; Review Group always includes appropriate VP's, Legal Services and Public Trust
7. Release package is reviewed and signed off by Delegated head (EVP, PSTD)
8. Any required briefings are completed by Public Trust (e.g., to Executive, Ministry)
9. Records are released on-time to the applicant by FOI team
10. If publication criteria is met, copy of redacted request is published to the BCER’s external corporate website

# Two-Phased Approach to FOI Process Improvements

## Phase 1 (Implemented)

- Establishment of an **internal FOI Review Group** to review/approve FOI release packages

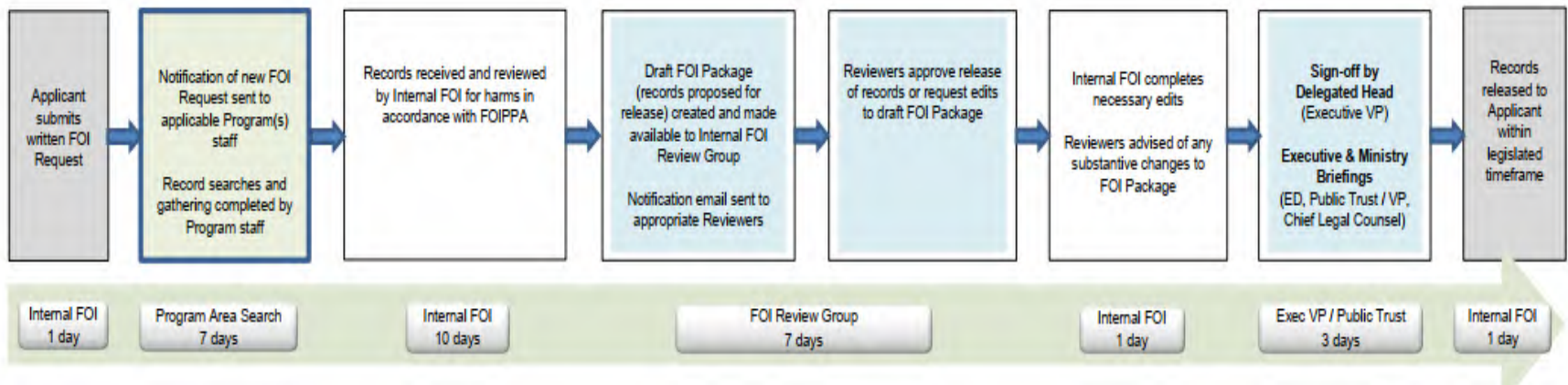
**Includes Leadership positions (VPs, EDs)** (approvals received via email)

- Establishment of a formal **sign-off process** (Delegation matrix)

## Phase 2 (To be implemented)

- Single point of contact model for FOI records searches
- Establish department (program) FOI contacts
- Contact receives notification emails of new FOI requests
- Contact coordinates records searches within their team
- Contact liaises with FOI and ensures responsive records are provided on time

# FOI Process Flowchart



# Phase 1 – Internal Review Group Implementation Benefits

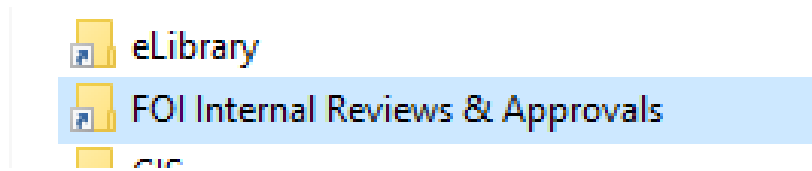
- Awareness of FOI requests relating to their areas
- “No surprises” – opportunity to review records and provide feedback prior to their release
- Reduced risk of sensitive information being released in error; or inappropriate withholding of information – programs know their business better than anyone
- Protects the Commissioner/BCER’s reputation – shared accountability approach (FOI/SMEs); formal process in place

# Review of FOI Release Packages

- Review Group is typically determined by program areas that have provided responsive records, with exception of Legal Services and Public Trust who review all requests
- If a request appears to have cross-organizational impact/interest, we'll notify all VPs and EDs as applicable of the request
- Release Packages relating to confidential personnel matters are sent to appropriate VP, Legal and Public Trust only for limited review

# Review and Approval Process – How does this work?

- Folder has been created on the K: Drive for FOI Release Packages requiring review



- All Release Package(s) requiring review and approval are saved here (except confidential personnel-related packages)
- VPs and Program Leads have access to this folder and its documents

# Review and Approval Process – How does this work (continued)?

- When a Release Package is ready for review and approval, a **notification email** from “FOI Intake” ([FOIIntake@bc-er.ca](mailto:FOIIntake@bc-er.ca)) is sent to the appropriate Review Group members
- VPs and EDs have option to include their program leads/SMEs in the review process
- Public Trust and Legal Services are copied on the notification email



# *Example:* Notification Email – “For Review and Comments”

S13

# What's Included in a FOI Release Package?

FOI Release Packages will include two items:

- **FOI Release Approval Form**
- **Redline** (records for release)

# FOI Release Approval Form

The **FOI Release Approval Form** provides an overview of the Request and supports sign-off

- Date request received
- Legislated due date
- Applicant type (industry, media, individual, etc.)
- Request wording (“Any and all records relating to...”)
- Comments/background notes (e.g., summary of any severing applied)
- Description of any 3<sup>rd</sup> party consultations completed (names of parties, what pages they were consulted on, whether their concerns, if any, were addressed through severing)
- BCER’s recommendation on release – e.g., Full disclosure, Partial disclosure, Access Denied...
- BCER’s recommendation on publication (based on established policy/criteria)

# “Redline” (Records for Release)

A **Redline** is a PDF (read-only) copy of all records deemed responsive to a request

- Pages may include **red boxes** around words, sentences or paragraphs
- This **redlining** is used to identify text deemed appropriate for redaction under FOIPPA; the FOIPPA section number that applies to the redaction is also visible

# *Example: "Redline"*

S13

# How Does the Internal Review Group approve an FOI Package?

- Simply reply to the original email that was sent by us ([FOIIntake@bc-er.ca](mailto:FOIIntake@bc-er.ca)) with...
- **“Approved” or “No concerns”**
- Copy of “Approval” email is saved in official FOI processing file
- Delegated Head will **not** sign-off until all required approvals have been received

# How Does the Internal Review Group Request Additional Severing, Ask Questions,

- Again, simply reply to the original email...
- If you think additional severing is required, please note in your reply the page number(s) and what text/info is harmful if released
- Please explain why - you don't need to quote a section of FOIPPA, just provide us with a rationale
- We'll try to support your severing requests, unless they're indefensible under FOIPPA
- If unable to support, we'll explain why not
- Any questions will be answered

# Consultation Requests from Other Public Bodies (Informal Process)

- Sometimes we receive “**Requests for Consultation**” from other public bodies
- Where another public body has received a FOI request, and within their release package are copies of records created by/pertaining to the BCER (e.g. emails between BCER/Ministry staff)
- Standard process is to provide us with an opportunity to comment on disclosure (e.g. is any severing required, or no concerns with release?)

## Different Process than FOI Requests (less formal/no sign-off):

- We email the records to appropriate staff for review/feedback (e.g. any harm with release?)
- Request details are provided: name of public body, request wording, applicant “type”, deadline for our response
- We then inform the other public body of the BCER’s views on disclosure – we ask to be informed if they’re not going to support our recommendations



# Internal FOI Team



Specialist, FOIPPA & Information Management:

– Dana Keough

Director, Records & Information Management:

– Mahia Frost

***BC'S FREEDOM OF  
INFORMATION AND  
PROTECTION OF PRIVACY  
ACT (FOIPPA)***

# OVERVIEW

- **FOIPPA APPLIES TO ALL PUBLIC BODIES IN BC.**
- **THE PURPOSE OF ACT IS TO MAKE PUBLIC BODIES MORE ACCOUNTABLE BY;**
  - **GIVING THE PUBLIC THE RIGHT OF ACCESS TO RECORDS;**
  - **SPECIFYING LIMITED EXCEPTIONS TO THE RIGHT OF ACCESS;**
  - **PROTECTING PERSONAL PRIVACY; AND**
  - **PROVIDING INDEPENDENT OVERSIGHT BY THE OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER (OIPC) OF ANY DECISIONS MADE UNDER THE ACT**
- **THE ACT APPLIES TO ALL RECORDS IN THE BC OIL AND GAS COMMISSION'S CUSTODY AND UNDER ITS CONTROL. THE COMMISSION IS RESPONSIBLE FOR THE SECURITY AND PROTECTION OF THESE RECORDS.**

# WHAT IS A RECORD?

- **A “RECORD” IS ANY INFORMATION RECORDED OR STORED WHETHER IN ELECTRONIC AND HARDCOPY FORMAT.**
- **THIS INCLUDES:**
  - **OIL & GAS APPLICATIONS**
  - **DOCUMENTS & REPORTS**
  - **MAPS, DRAWINGS & PHOTOGRAPHS**
  - **LETTERS & WRITTEN CORRESPONDENCE**
  - **EMAILS**
  - **TELEPHONE RECORDS**
  - **NOTE BOOKS, ETC.**

# DUTY TO ASSIST

**WHEN AN FOI REQUEST IS RECEIVED BY THE COMMISSION, IT HAS THE DUTY TO ASSIST. THIS MEANS THE COMMISSION MUST:**

- **MAKE EVERY REASONABLE EFFORT TO ASSIST APPLICANTS;**
- **RESPOND OPENLY, ACCURATELY AND COMPLETELY TO REQUESTS WITHIN THE 30 DAY TIMELINE OR LIMITED EXTENSION PERIOD;**
- **CONDUCT AN ADEQUATE SEARCH FOR RECORDS; AND**
- **IN LIMITED CIRCUMSTANCES, CREATE A RECORD WHERE THE DATA EXISTS.**



# LEGISLATION



## **OIL & GAS ACTIVITIES ACT GENERAL REGULATION**

- **S. 17.1(c) – APPLICATIONS AND AMENDMENTS FOR PERMITS, INCLUDING ALL SUBMISSIONS SUPPORTING THE APPLICATIONS**

## **FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT EXCEPTIONS TO DISCLOSURE:**

- **S. 16 – DISCLOSURE HARMFUL TO INTERGOVERNMENTAL RELATIONS OR NEGOTIATIONS:**
  - **NEGOTIATION & CONSULTATION WITH FIRST NATIONS IN RELATION TO SPECIFIC APPLICATIONS;**
  - **ALL OF THE COMMISSION’S COMMUNICATIONS WITH INDIGENOUS COMMUNITIES THROUGHOUT THE PROVINCE;**
  - **FINANCIAL AGREEMENTS & RECORDS OF PAYMENTS.**
- **S. 18 – DISCLOSURE HARMFUL TO THE CONSERVATION OF HERITAGE SITES:**
  - **ARCHAEOLOGY DATA;**
  - **HERITAGE SITES.**
- **S. 22 – DISCLOSURE HARMFUL TO PERSONAL PRIVACY:**
  - **INDIVIDUAL NAMES, ADDRESSES, PHONE NUMBERS**
  - **CONSULTATION WITH LANDOWNERS OR OTHER STAKEHOLDERS**

# COMMISSION PRIVACY PRACTICES

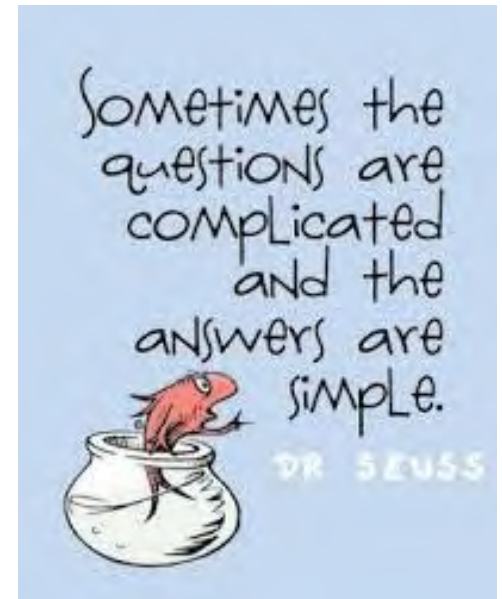
- **ALL RECORDS ARE SUBJECT TO FOI;**
- **JUST BECAUSE IT IS REQUESTED DOES NOT MEAN IT WILL BE RELEASED;**
- **THE COMMISSION IS COMMITTED TO PROTECTING PERSONAL PRIVACY;**
- **THE COMMISSION CONSIDERS CONSULTATION AND NEGOTIATION RECORDS WITH INDIGENOUS COMMUNITIES CONFIDENTIAL AND DOES NOT DISCLOSE THESE RECORDS TO THIRD PARTIES;**
- **ONLY GENERAL INFORMATION IS PUBLICLY AVAILABLE ON THE COMMISSION'S WEBSITE SUCH AS BCOGC CONSULTATION AREAS, CONSULTATION AND LONG TERM OIL & GAS AGREEMENTS;**
- **THE COMMISSION ENSURES IT HAS MEASURES IN PLACE TO PREVENT THE UNAUTHORIZED COLLECTION, USE AND DISCLOSURE OF PERSONAL AND CONFIDENTIAL INFORMATION.**

# HELPFUL LINKS

- **FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT**
  - [HTTP://WWW.BCLAWS.CA/RECON/DOCUMENT/ID/FREESIDE/96165\\_00](http://www.bclaws.ca/recon/document/id/freeside/96165_00)
- **OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER**
  - [HTTPS://WWW.OIPC.BC.CA/](https://www.oipc.bc.ca/)



# Any Questions



# RECORDS MANAGEMENT & FOI

## Records and Information Services (RIS)

Dana Keough and Mahia Frost



# Records and Information Services

Our Role

EE Resources

Projects



## Records & Information Services

Welcome to the Records and Information Services (RIS) space. The RIS team is responsible for Information Management (IM), Freedom of Information (FOI) and Protection of Privacy.

**Our vision:**

We have an information management program of excellence.

Our program enables the BC Energy Regulator to fulfill its mandate, facilitate legislative and policy compliance, provide good stewardship of our information, and support service delivery to citizens.

Our staff understand how we manage Regulator information, their responsibilities, and our processes.

**Our mission:**

We deliver an efficient and effective Information Management program and services to support the mandate of the BC Energy Regulator and its compliance requirements.



Information Management Resources



Freedom of Information (FOI) and Protection of Privacy

926/Mcas/Ctx=4

## ORCS / Shared Drive Organization Projects / SharePoint

Information Management Act requirements

ARCS / ORCS – Records Classification systems

OGC Shared Drive Organization Projects

SharePoint Projects



## Freedom of Information & Protection of Privacy Act (FOIPPA)

FOIPPA is provincial legislation that applies to all public bodies in BC.

The purpose of the Act is to make public bodies more accountable by:

- Giving the public the right of access to records;
- Specifying limited exceptions to disclosure;
- Protecting personal privacy;
- Preventing the unauthorized collection, use or disclosure of personal information; and
- Providing independent review of decisions made under the Act.

The Act applies to all records in the BCER's custody and under its control. The BCER is responsible for the security and protection of these records.



## What is a Record?

A “record” is any information recorded or stored whether in electronic, hardcopy or other format.

Examples include:

- Oil & gas activity & application files (such as well, pipeline, facility (LNG), road, ancillary)
- Spatial data (GIS)
- Documents & reports
- Maps, drawings & photographs
- Letters & written correspondence
- Emails, messaging apps, text messages
- Telephone records
- Notebooks, handwritten notes, etc.

## What is FOI-able?

- All BCER records, data and information fall within the scope of the Act and can be FOI'd
- Just because records are requested does not mean they will be disclosed.
- Confidential or sensitive information and data are protected from disclosure pursuant to applicable legislation and FOIPPA exceptions.
- Be aware that just because it's embarrassing does not mean it will be withheld or severed from responsive documents. Records can only be severed or withheld in accordance with the exceptions outlined in FOIPPA
- Disclosure should be the rule, not the exception
- If you are unsure, don't be afraid to ask questions!

## BCER FOI Process

Where proactive disclosure is not possible, a formal written request is required:

- BCER receives FOI request and sends an acknowledgement letter to applicant and the 30-day timeline starts
- A call for records is sent out to program areas and responsive records are gathered
- Records are combined and collated into a PDF package
- A line-by-line review is conducted for harms and a redline package is created:
  - A **redline** is a PDF copy of all records deemed responsive to the request. Pages contains red boxes around sections that are recommended for redaction or severing of the information in accordance with FOIPPA.
  - This could include information where disclosure is harmful to law enforcement, business interests of a third party, personal privacy, conservation of heritage archaeology sites, or consultation with Indigenous peoples and landowners or other sections of the Act.
- Redline package is circulated for VP, SME, and legal review/sign off and approval
- Delegated head signs off
- Final severing/redactions are applied and a final release package is prepared and released to the applicant



## Tips for Good Privacy Practices

- Always be professional in your written communications
- When writing reports, state facts rather than personal opinions
- Use generalized terms/statements rather than directly identifying individuals, and limit personal information
- Have verbal conversations with colleagues to discuss facts prior to putting it in writing;
- Delete or destroy transitory records;
- Make time to delete and clean out your email accounts, including archives, deleted folder or other folders;
- Remove personal or junk emails;
- Review your communications prior to sending;
- Limit collection of personal information;
- Ensure good security measures are in place for the protection of sensitive and confidential information.

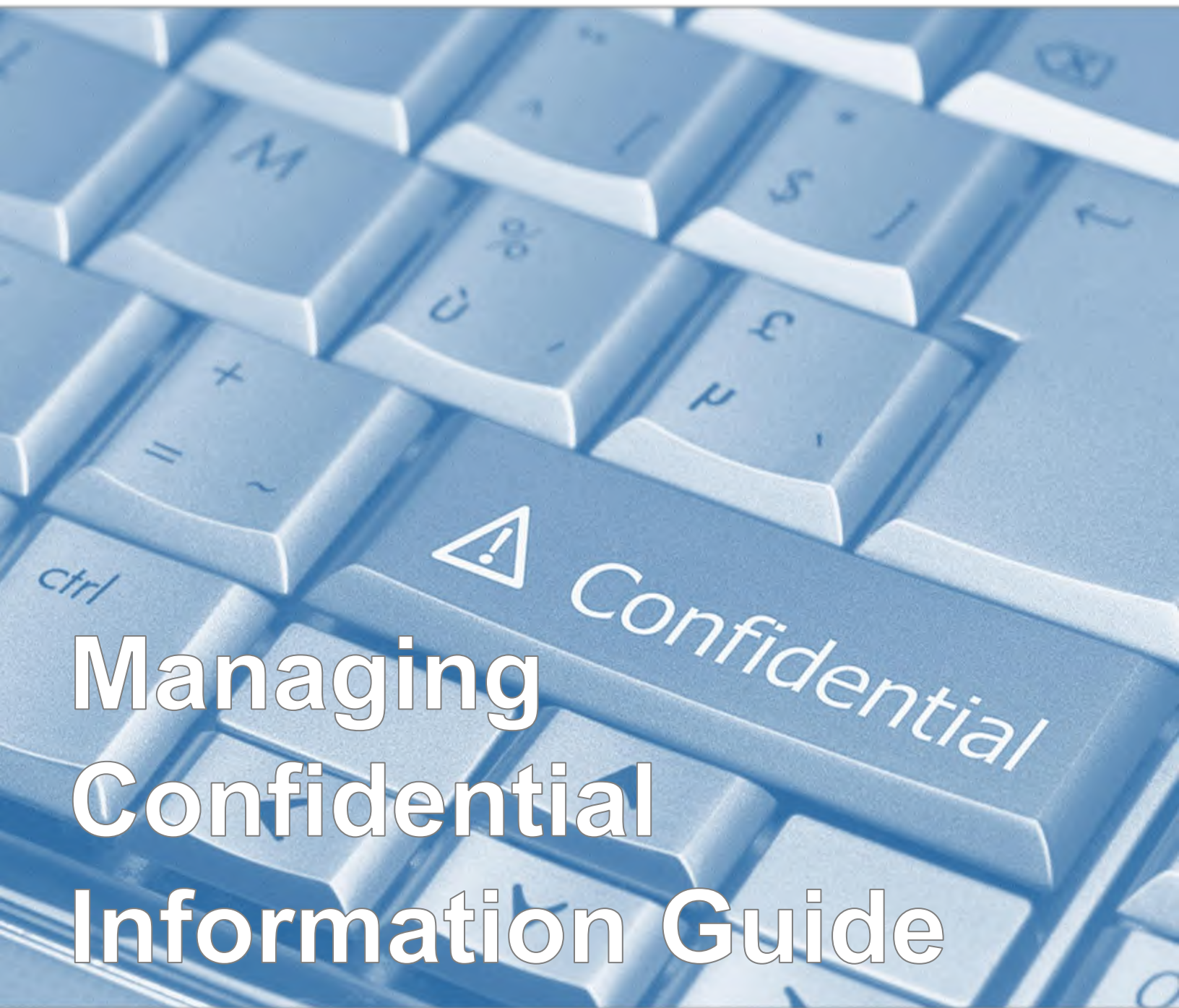
# Any Questions

The title 'Any Questions' is presented in a playful, bubbly font. 'Any' is in white with a blue outline, and 'Questions' is in a bright yellow-green with a blue outline. To the right of the text is a black and white icon of a speech bubble with a question mark inside. The entire graphic is set against a light blue, cloud-like background.

Sometimes the  
questions are  
complicated  
and the  
answers are  
simple.



DR SEUSS



**Managing  
Confidential  
Information Guide**

June 2023

# Table of Contents

Overview	3
Understanding Confidentiality	4
Basic Do's and Don'ts	5
In the Workplace	6
Outside the Workplace	7
Maintaining Confidentiality	8
Information Disposition	9
Pop Quiz!	10
Policies	12
Contacts	12

*This guide is the result of collaboration between the Executive Vice Presidents and key staff from Legal Services; Public Trust; Information Systems and Technology; and Records and Information Services.*

# Overview

Information is one of an organization's most valuable assets. In the course of conducting business, BC Energy Regulator (BCER) employees often handle information that is sensitive due to confidentiality reasons or other obligations.

---

Confidential information is information that, if compromised, could result in serious consequences for individuals, organizations, or government. Designating information as confidential depends on factors such as the value of the information, the source of the information, and the impacts of unauthorized use, disclosure, alteration, reproduction, loss or destruction.

---

All BCER employees (which includes all staff levels, contractors, and students working with the BCER) have a responsibility to appropriately manage and protect confidential information, regardless of whether they are the creator or recipient of the information. The public, industry, Indigenous communities and other government agencies regularly entrust the BCER with confidential information and rely on us to keep it safe while it is in our custody and control.

This guide has been created to assist BCER employees in securing:

- Our workplace.
- The information (sometimes referred to as data, documents, records, content) we create, receive and manage on behalf of the Province of British Columbia.

By consistently practicing a few simple habits, we can ensure confidential information is safeguarded.

# Understanding Confidentiality

You may be unclear whether the information you have is confidential or not. The following questions are considered when assessing information for disclosure under the Freedom of Information and Protection of Privacy Act (FOIPPA) and may help you in determining confidentiality.

**If the answer to any of these questions is yes, then the information may be confidential** and require appropriate management. If you are unsure, discuss with your supervisor.

## Does the information:

- Contain confidential consultation with other government bodies?
- Relate to economic policies/activities for which we are responsible? Or, contain a monetary value that is not public?
- Relate to administrative or personnel management plans that are not yet public?
- Contain information about a business's confidential negotiations with the BCER?
- Reveal a company's trade secrets?
- Contain legal advice or relate to a legal matter?
- Relate to records submitted, or prepared for submission, to Cabinet? Treasury Board?
- Contain policy advice prepared for the BCER or another public body?
- Consist of draft materials / advice / recommended courses of action?
- Have a legislative requirement concerning a period of confidentiality (such as well data)?
- Contain personal information relating to, about, or from individuals (e.g. personal opinions collected through a consultation process)?

## More ways to look at it:

- Was the information supplied in confidence?
- Could release of the information harm a company's competitive position, result in the BCER no longer receiving the information, or result in undue financial losses or gains?
- Could release of the information harm our relationship with the Province, any of its agencies or other governments (i.e. other provinces, federal, indigenous, municipal, etc.)? Is the information ours to release (do we have the greater interest)? Or, could the timing of release have a negative impact on another public body or government?



# Basic Do's and Don'ts

- Remember your affirmation of the BCER's **Employee Code of Conduct and Ethics**.
- Maintain a “clean desk” and always lock your computer (Windows Key + L) when you are away from your desk.
- Use the provided locked shredding bins whenever you are disposing of **transitory** confidential information (paper) in the office. Do not dispose of BCER information in recycling containers.
- Do not disclose BCER information, regardless of its sensitivity, without appropriate authorization.
- Use <https://forgetmenot.bcogc.ca/> to store your BCER passwords. Do not write them down on sticky notes, store them under your keyboard, etc.
- Do not discuss or review confidential information in open work spaces, public areas, or when using public Wi-Fi.



## Why this is Important

Protects the relationship of trust that is necessary for an effective working relationship between the BCER and our external partners (i.e. ministries, industry, educational institutions, Indigenous communities), and within our organization.

# In the Workplace

## Access

Security starts at the front door. Managing who gets into your workplace is an essential protection for confidential information. Follow these simple practices to prevent unauthorized access:

- If you see someone you do not know in your area or waiting at an access point, politely ask if you can help (if you are comfortable doing so).
- Do not let people follow you through access points if you do not know them.
- Report doors that do not close properly to your supervisor or Corporate Property and Administration.
- Ensure visitors to our workplace are signed in, and are accompanied by a BCER employee.

## Your Workspace

Developing and implementing security-conscious work habits will reduce the likelihood of someone seeing or disclosing confidential information. Employees are expected to take reasonable steps to ensure the security of information they are creating or that is in their custody. Your practices should include:

- Locking your computer when you leave your desk to prevent unauthorized users from accessing the BCER's network and/or information.
- Securing sensitive documents in a locked drawer or cabinet.
- Maintaining a clean desk practice.

## Clean Desk Practice

Remember to clear desks, workstations or work surfaces and secure all information prior to leaving the work area unattended:

- Clear your desks, workstations/surfaces, etc. of all confidential information at the end of each day, and secure the materials in provided storage spaces, or ensure your office door is locked.
- Take reasonable steps to safeguard BCER-issued IT assets and confidential information.
- Report any actual or suspected information security and/or privacy breaches immediately to your supervisor, the Director, Information Security (in the case of a data/network security breach), and the Director, Records & Information Management and Specialist, FOIPPA (BCER's designated Privacy Officers) if a breach relates to loss, theft or disclosure of personal information.



# Outside the Workplace

Secure Remote Access Services (VPN) are provided by the BCER to ensure a secure connection to the network when working remotely. Once connected, you will be able to access the same network resources (e.g., shared drives) the way you normally would in a BCER office.

To ensure your information remains secure outside the workplace, take the following steps:

- Do not forward BCER information to personal accounts (e.g., Dropbox, Gmail, Google Drive, etc.).
  - Use only BCER-issued devices (laptops, smartphones, USB keys, etc.) for BCER work and for remote access to our network. BCER-issued devices offer security features, such as encryption, password protection, and the ability to be wiped remotely if lost or stolen.
- Do not use personal email or messaging (texting) accounts to carry out BCER business.
  - If this happens in an extenuating circumstance, you must copy the email(s) to your BCER email address or transcribe the text message into a document (e.g. word document), and delete the information from your personal account as soon as possible; ensure you share the least amount of information that is necessary in the circumstance.
- Avoid storing or transporting sensitive information on mobile devices. If an exception is required, please consult with your supervisor. Only use BCER-issued encrypted portable storage devices, and only as needed.
- In cases where mobile devices must be used to conduct BCER work, use strong passwords and do not share them with anyone else. Adopt good security practices for selecting passwords as outlined in the BCER's [Information Security Policy](#).
- If you travel with physical documents, only take what is necessary for the job and make sure you have appropriate approval to transport the material.
- Protect confidential information while in transit or outside the office; do not leave mobile devices or confidential documents unattended or in plain view (for example, in the backseat of your car, etc.).
- When using remote access services, avoid public Wi-Fi and ensure you are the only one who works on your BCER-issued computer.
- Take appropriate measures to prevent others from overhearing or viewing confidential information, including ensuring your screen is not visible by others, preventing others from looking over your shoulder, and finding a private place to take a phone call.

# Maintaining Confidentiality

The BCER aspires to uphold the highest standards in maintaining confidentiality and professional integrity.

Employees are required to affirm the **Employee Code of Conduct and Ethics** annually; it is a condition of employment. The Code of Conduct requires you to maintain the confidentiality of information or documents that come into your possession, or you have knowledge of in your role as a public servant. It also outlines the consequences of failing to do so. Please ensure you fully understand the responsibilities associated with maintaining confidentiality.

The requirement to comply with the BCER's Code of Conduct is a condition of employment. Please ensure you fully understand the responsibilities associated with maintaining confidentiality, as there are consequences of failing to do so. Possible consequences of non-compliance are outlined within the Code.

## BC Energy Regulator's Employee Code of Conduct and Ethics:

### **Confidentiality**

Confidential information, in any form, that employees receive through their employment must not be disclosed, released, or transmitted to anyone other than persons who are authorized to receive the information. Employees with care or control of personal or sensitive information, electronic media, or devices must handle and dispose of these appropriately. Employees who are in doubt as to whether certain information is confidential must ask the appropriate authority before disclosing, releasing, or transmitting it.

The proper handling and protection of confidential information is applicable both within and outside of BCER and continues to apply after the employment relationship ends.

Confidential information that employees receive through their employment must not be used by an employee for the purpose of furthering any private interest, or as a means of making personal gains.

### **Why this is Important**

Protects the legal and business interests of the government and affected stakeholders.

# Information Disposition

## The same rules apply to confidential information.

BCER information, regardless of its format or sensitivity, must be disposed of in accordance with approved records retention and disposition schedules. These schedules are legal authorities that specify how long records are to be kept, and their final disposition (destruction or archival preservation).

Some information BCER employees create or receive may be considered transitory and should be handled accordingly. The following resources offer additional guidance:

- [Transitory Records Guide](#)
- [Official vs. Transitory Records](#)

Information that is subject to legal activity or requested under the Freedom of Information and Protection of Privacy Act (FOIPPA) cannot be disposed of until the matter has been resolved or the request completed. For more information on the types of information protected by FOIPPA, please contact one of the BCER's FOIPPA Specialists.



### Why this is Important

Protects confidential or sensitive information that is often accessible to us as part of our work, and for which we are the trusted stewards.

# Pop Quiz!

1. Which of these record types could contain confidential information?
  - Text messages
  - Draft briefing notes
  - Databases
  - Meeting handouts
  - Emails
2. Where should you dispose of transitory physical documents?
  - Recycling bins
  - Locked shredding bins
3. Should confidential information be disposed of when you are finished using it?
  - Yes
  - No
  - It depends
4. Is it okay to use your home email to do your work?
  - Yes
  - No
  - It depends
5. I work better with my coloured file folders holding my documents on my desk. Our office is secure, can't I just leave my stuff out and easy to find?
  - Yes
  - No
  - It depends
6. I am travelling between Kelowna and Fort St. John a lot these days. My personal USB device holds more documents than the BCER one – can't I just use that while doing this project?
  - Yes
  - No
  - It depends

Answers on the next page...

## Pop Quiz Answer Key:

1. All of them! All of these records are considered government information, and any of them “could” contain confidential information. It doesn’t matter what medium is used to produce a record, what makes it confidential is the context and the content.
2. In the locked shredding bins. BCER information should never be processed through recycling bins.
3. It depends. If the information is transitory then it may be shredded, or deleted, but if it’s a record that you have used in making a decision, or if it records a working activity, then it must be managed according to the retention as outlined in our records classification systems. Please see our [Official vs. Transitory](#) records guide for clarity. And remember! Transitory information is subject to FOIPPA requests and may not be deleted if a request is open/active.
4. No. Do not use your home email to conduct BCER business. The BCER provides secure transmission and servers to protect the information we use to conduct our business.
5. Not if the information is confidential. Best practice recommends you clear your desk every evening, so you don’t accidentally leave confidential material out.
6. No. The BCER issues encrypted USB drives for when you must carry documents on a portable storage device. If you are carrying BCER information, you must use a BCER-issued device. And remember to remove the records off the device and into the BCER storage environment when you aren’t requiring mobile access!

# Policies

- ✓ [Building Access and Security policy](#)
- ✓ [Information Management Policy](#)
- ✓ [Information Security Policy](#)
- ✓ [Mobile Device Policy](#)
- ✓ [Use of IT Resources Policy](#)
- ✓ [Workplace Appropriate Use Policy](#)

# Contacts

If you would like more information regarding what is in this guide or wish to report an incident, please refer to the table below.

Commission Contact	When to Contact	Email
Corporate Property and Administration <a href="#">Corporate Property and Administration Resources</a>	For general inquiries, or to report a facility or security breach.	<a href="mailto:servicedesk@bc-er.ca">servicedesk@bc-er.ca</a>
Records and Information Services (Records Management) <a href="#">Information Management Resources</a>	For general inquiries on how to manage government information.	S17
Records and Information Services (FOIPPA and Privacy) <a href="#">FOIPPA and Protection of Privacy Resources</a>	For general inquiries, or to report a privacy breach.	
IT Service Desk <a href="#">Service Desk</a>	For technical support or ensuring your mobile device is encrypted.	<a href="mailto:servicedesk@bc-er.ca">servicedesk@bc-er.ca</a>
Information Security/Cybersecurity <a href="#">Cybersecurity Resources</a>	For general inquiries, or to report an incident of phishing, cybersecurity attacks, or a data/network breach.	<a href="mailto:servicedesk@bc-er.ca">servicedesk@bc-er.ca</a>
Human Resources and Workplace <a href="#">Code of Conduct and Ethics Page</a>	For general inquiries about the Code of Conduct and Ethics.	<a href="mailto:servicedesk@bc-er.ca">servicedesk@bc-er.ca</a>



# Managing Transitory Information Guide

# Table of Contents

How can I identify Transitory Information? .....	3
What are my Transitory Information responsibilities? .....	4
Common categories of Transitory Information.....	5
<b>1 Transitory messages</b> .....	5
<b>2 Transitory drafts</b> .....	5
<b>3 Rough notes and working materials</b> .....	6
<b>4 Transitory copies</b> .....	6
<b>5 Transitory systems information</b> .....	7
<b>6 Transitory Information from external sources</b> .....	8
Examples of information that is NOT transitory .....	9
Contacts .....	10

*This guide is based on the BC Government Transitory Information Guide.*



Not all Commission information needs to be retained. This guide provides in-depth assistance to help you identify information that is transitory and understand the requirements of the [Transitory Information Schedule](#). If all you need is the basics, refer to [our Transitory Information Quick Tips Guide](#).

## How can I identify Transitory Information?

Individual employees do not need formal authorization to destroy transitory information, so long as the records are not needed for a Freedom of Information (FOI) request or legal search, and the destruction is secure. However, employees sometimes do need help determining whether information is transitory or not.

There are a series of documents to help you understand what transitory information is:

- The [Transitory Information Schedule](#) defines and categorizes transitory information and establishes retention and disposition requirements for it.
- The [Quick Tips Guide](#) summarizes what is and is not transitory information.
- **This guide** provides an analysis and examples of transitory information categories, finishing with a table of examples of information that is NOT transitory.

Most transitory information is easy to identify because it has not been filed and is not needed for any reason. Some information is harder to assess, especially after relevant actions are completed. Content and context determine whether information is transitory, not its format or medium. If an email, handwritten note, draft, or copy is essential to understanding Commission business (e.g., how a decision was reached or program delivered), then the record must be kept, and is not transitory.

Records that are scheduled and classified by ARCS or ORCS and/or filed in the office recordkeeping system are never transitory. They need to be managed appropriately and securely destroyed in accordance with Commission requirements (see our [Information Management Policy](#) and the [Documented Destruction Process Overview](#))

# What are my Transitory Information responsibilities?

Both the [Transitory Information Schedule](#) and the Commission's [Use of IT Resources Policy](#) require employees to:

- dispose of transitory information that they are responsible for when it is no longer needed,
- ensure that the information is not relevant to a FOI request or request for legal discovery before proceeding with destruction, and
- always ensure that destruction occurs in a secure and confidential manner.

As an employee of the Commission, you need to be able to distinguish transitory information from records and data that document business decisions and actions. Routinely deleting transitory information ensures that the Commission is storing and managing the information it needs to keep.

## Documenting Decisions

If your information contains evidence of actions or decisions, it must be managed as a record in the appropriate recordkeeping system. See

[Documenting Commission Decisions](#)

# Common categories of Transitory Information



Transitory Information includes, but is not limited to, records that are identified and described in the following common categories.

## 1 Transitory messages

Transitory messages are casual or non-substantive messages, in any format and including attachments, that are of only short-term use and are not needed to document an action or decision. They can take many forms (e.g., email, instant messages, chat messages in online collaboration tools, social media postings, facsimile [fax], voice/video message recordings).

Messages or attachments that are required for ongoing business needs are not transitory information. Due to their content or context, they must be retained (e.g., email documenting a policy decision, formal memo about Commission business, social media post that is the initial announcement of a new program). However, once these have been saved into an appropriate recordkeeping system, any additional copies of the messages may be considered transitory copies (see section 4).

### Examples of transitory messages

- announcements of social events
- cc copies (unless you are the main staff member responsible for the matter)
- emails conveying an attachment (if it doesn't add value to the attachment)
- meeting arrangements
- routine correspondence about drafts and revisions
- requests to call someone

## 2 Transitory drafts

Transitory drafts are preliminary or incomplete drafts that do not contain significant annotations, comments, approvals, or substantial changes providing insight into the evolution of the final version. Once a subsequent draft or finished record has been developed and filed, these drafts are no longer needed.

### Is this draft transitory or not?

- Is it complete/final?
- Is this the latest version available (i.e. it hasn't been replaced by a new version)?
- Was this draft used for formal consultation and review?
- Does it document a decision or approval?
- Does it represent a substantial revision?
- Is this draft subject to legislative, policy, or information schedule requirements?

**If you answer “YES” to any of these questions, keep the draft, it is NOT transitory.**

## Examples of transitory drafts

- preliminary drafts that were never reviewed
- interim drafts that reflect minor editorial changes

### 3 Rough notes and working materials

Rough notes and working materials consist of preliminary, incomplete, or unused information maintained for the purposes of creating other documents, aiding memory, facilitating a routine action, or recording exploratory thoughts. They include documentation used to support projects and develop official records, often generated during brainstorming and collaboration activities.

Context and content affect the value of these records. If rough notes or other working materials help to illustrate a key decision-making process, particularly if the decision affected an individual, it is necessary to file and retain them (see [CRO Directive 01-2019: Documenting Government decisions](#)). Where subsequent or final records exist, however, the rough notes do not need to be kept, unless there is some other reason for doing so.

## Examples of transitory rough notes and working materials

- outlines, calculations, summaries, flipcharts, and other rough notes not needed to support projects
- preliminary notes and working materials used to prepare a final record
- failed job output records resulting from abnormally ended jobs, programming errors, improper selection criteria, or unsuccessful data input

### 4 Transitory copies

Transitory copies are duplicates of existing records made for convenience or reference. These copies are not authoritative copies needed to replace originals as evidence of actions, decisions, or consultation. The following types of copies are transitory information:

- a) Extra copies of records where the authoritative copy/original record has already been saved in an appropriate recordkeeping system. These include:
  - convenience copies
  - partial copies/extracts
  - copies made to support computer processing functions
  - copies used to support the development of other documents
- b) Output from electronic systems created for reference purposes
- c) Supplies of Commission publications and forms/templates (not including the official file copy of the publication/form/template or completed forms)

Copies kept for reference purposes may be classified under [ARCS 358-20 Library/topical reference materials](#).

## Examples of transitory copies

- copies created for convenience (e.g. agendas printed for use at a meeting)
- automatically generated copies of a master file that are no longer needed (e.g., processing/transmittal copies, user views that can be reconstituted)
- supplies not distributed (e.g., forms, pamphlets, newsletters, reports)

## 5 Transitory systems information

Transitory systems documentation consists of information of temporary usefulness generated for, or resulting from, computer systems operations (also known as transitory electronic data processing [EDP] records). It includes:

- a) Input source documents used to enter information into a digital system (e.g., data entry forms), after which it is no longer needed
- b) Automatically gathered/generated data processing information, including:
  - Data processing information generated in the process of transferring data between systems, obsolete after transfer is completed and validated
  - System output/reports generated for reference or for a client, not needed as part of a file or for system maintenance
  - Internet browsing documentation (e.g. browsing history, cookies, cache/temporary files)
- c) Unneeded documentation of systems and internet usage.

Transitory systems documentation excludes data in the systems. Data that has been migrated or converted and thereby rendered redundant is covered by the Redundant Source Information Schedule, section 3.

NOTE: Systems documentation that is needed for operational purposes, ongoing maintenance, or for purposes of an investigation, is not transitory and should be retained in accordance with ARCS (see primaries [6450 Information System Development and Changes](#) and [470 Security Management](#)) or the appropriate ORCS.

## Examples of transitory systems information

- data entry forms and EDP records not needed after the information is entered into a system
- internet browsing information (e.g., cookies, temporary internet files)
- data from connected devices that is not used, or is duplicated/ summarized in reports)
- empty folders and zero-byte files that have no further use
- notes, forms, and other input source documents used for data entry

## 6 Transitory Information from external sources

Transitory information from external sources includes solicited and unsolicited information from external sources that has been used solely for short-term reference purposes or not at all, including:

- a) **Extracts or copies** of publications, promotional material, and other material from external sources.
- b) **Unsolicited information** that is not used by the receiving office but may be redirected to the appropriate government body.
- c) **Solicited and unsolicited information that is confidential in nature and is not needed to document a commission action or decision.**

NOTE: It is important to promptly and securely destroy or return any transitory information that contains personal or other confidential information that is not used by the receiving office, including:

- information identified as confidential in legislation or policy, as well as
- information that may not normally be recognized as confidential, except in relation to specific groups such as Indigenous communities.

The provision to securely return information to the sender has been included in the Transitory Information Schedule and in this guide to allow for this to happen when it is necessary and appropriate, in accordance with relevant legislation, policy, or the needs of the sender. (Please note that it is not the action of returning the information to the sender that renders it transitory. If a copy is needed for the Commission to take an action or make a decision, that copy should be retained in the appropriate recordkeeping system, even after the original is returned to the sender.)

Published items that are used as part of a procurement process or other transaction are **not** transitory.

### Examples of Transitory Information from external sources

- advertising and promotional material not used for procurement or other transactions (e.g. spam, junk mail, catalogues, promotional DVDs, course announcements)
- newspapers or magazines used to compile news clippings relevant to a program area (the actual news clippings are filed under [ARCS 295-04](#))
- unsolicited correspondence from the private sector that is not used for any actions or decisions
- information provided in confidence that is forwarded to the appropriate government body or returned to the sender, and not used by the Commission

# Examples of information that is NOT transitory



## Evidence

- drafts or revisions with information that is not documented elsewhere (e.g., directions to change a proposal or a course of action)
- draft legislation (file under [ARCS 140-20](#))
- draft audit reports kept to comply with policy
- legal advice and agreements
- unread emails that are evidence of attempted consultation

## Documenting Decisions & Actions

- business transactions documentation (initiation, authorization, or completion)
- records that include instructions, approvals and advice
- emails that document a policy, decision, significant action, or how a case was managed
- records that help explain the history of a relationship, decision or project

## Operational Needs

- data that is needed for ongoing business
- information that is integral to a file about one event, client, or issue (i.e., a case file)
- reference material with ongoing value to the office
- work unit activities documentation (e.g. work schedules, assignments)

## Official Communications

- formal communication about Commission business
- social media post officially announcing a new Commission program

## Official/Final Records

- final reports and recommendations
- official copies of agendas and minutes
- official copies of policies, directives, procedures, standards, guides
- signed briefing notes

## DO NOT destroy any transitory information that:

- may be relevant to a current/anticipated FOI request or legal discovery, or
- is stored in backup systems, which are an essential part of protecting the Commission's information assets (i.e. "triple deleting" is not allowed).

## Policies

- ✓ [Employee Code of Conduct and Ethics](#)
- ✓ [Information Management Policy](#)
- ✓ [Use of IT Resources Policy](#)

## Contacts

If you would like more information regarding what is in this guide or wish to report an incident, please refer to the table below.

Commission Contact	When to Contact	Email
Records and Information Services (Records Management)  <a href="#">OGC Information Management Page</a>	For general inquiries on how to manage commission information.	<a href="mailto:servicedesk@bcogc.ca">servicedesk@bcogc.ca</a>
IT Service Desk <a href="#">Service Desk</a>	For technical support.	<a href="mailto:servicedesk@bcogc.ca">servicedesk@bcogc.ca</a>



# INFORMATION MANAGEMENT 101

## Transitory Information

Presenter: Mahia Frost  
Records and Information Services





## Objective



For you to gain a better understanding of transitory information, and why this is an essential element in managing BCER information.

## IM Framework in BCER



Information Management Act

Freedom of Information and  
Protection of Privacy Act

Professional Governance Act

Information Management  
Policy

Documenting Government  
Decisions Directive

ARCS/ORCS/Transitory  
Information Schedule



**Legislation and Policy**

## Definition – Record

### INTERPRETATION ACT [RSBC 1996] CHAPTER 238



**"record"** includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise;



## Transitory Information



1. Transitory messages
2. Transitory drafts
3. Rough notes and working materials
4. Transitory copies
5. Transitory systems information
6. Transitory information from external sources

All quite common sense – records of low value and temporary usefulness

## Category 1: Transitory messages

Messages and attachments that do not document a business activity or decision (i.e., message content lacks substance).

- Correspondence about meetings
- Announcement of a social event
- “cc” and “FYI” messages (unless you are the main staff member responsible for the matter)
- Routine message about drafts and revisions
- Emails conveying an attachment (if it doesn’t add value to the attachment)

## Category 2: Transitory drafts

Drafts with no significant annotations, comments, approvals, or substantial changes; **i.e.** preliminary drafts that were never reviewed or interim drafts that reflect minor editorial changes

### Is this draft transitory or not?

- Is it complete/final?
- Is this the latest version available (i.e., it hasn't been replaced by a new version)?
- Was this draft used for formal consultation and review?
- Does it document a decision or approval?
- Does it represent a substantial revision?
- Is this draft subject to legislative, policy, or information schedule requirements?

**If you answer “YES” to any of these questions, keep the draft, it is NOT transitory.**

## Category 3: Rough notes and working materials

Information used to support projects and develop official records.

- Flipchart pages (and other brainstorming records)
- Outlines, calculations, summaries, and other rough notes not needed to support projects
- List of ideas or suggestions
- Preliminary notes and working materials used to prepare a final record



## Category 4: Transitory copies

Copies not needed as evidence of decisions, actions, or consultation.

- Extra copies of records where the official copy/original record has already been saved in an appropriate recordkeeping system.
- Output from electronic systems created for reference purposes
- Copies created for convenience (e.g. agendas printed for use at a meeting)
- Supplies not distributed (e.g., forms, pamphlets, newsletters, reports)
- Partial copy / extracts

## Category 5: Transitory systems information

Information that is no longer needed after it is entered into systems or generated as output.

Unneeded systems and internet usage documentation.

- Internet browsing information (e.g., cookies, temporary internet files)
- Data input forms
- System output created for reference or for providing to clients

## Category 6: Transitory information from external sources

Published, solicited and unsolicited items that have been only used for reference, referred to another office, or returned to sender

- Advertising in various formats
- Newspapers and magazines
- Spam or junk mail
- Unsolicited correspondence not used for any actions or decisions
- Information redirected to the appropriate office (such as a forwarded email)
- Confidential information returned to sender (unless used by the BCER to take an action or make a decision)

## Summary of Transitory Information



- Common sense rules
- You, as the expert in your work, can make the decision
- You can delete when your use is complete
- Clears the way to focus on managing the records that have value.



### **Important Caveat**

**Do not destroy transitory information that may be relevant to a Freedom of Information (FOI) request or legal discovery.**

## What is not transitory



Consider if the record is:

- Required to document a decision
- Required to meet legal or financial obligations
- Needed to sustain BCER operations, programs, or administration
- Integral to a case (i.e., needed as context for related records)
- Needed for accountability purposes
- Covered by ARCS or ORCS

**If you answer “YES” to any of these questions, the record is NOT transitory.**

# Examples of what is NOT transitory

These are official records and should be filed into the recordkeeping system.

## Evidence

- drafts or revisions with information that is not documented elsewhere (e.g., directions to change a proposal or a course of action)
- draft legislation (file under [ARCS 140-20](#))
- draft audit reports kept to comply with policy
- legal advice and agreements
- unread emails that are evidence of attempted consultation

## Documenting Decisions & Actions

- business transactions documentation (initiation, authorization, or completion)
- records that include instructions, [approvals](#) and advice
- emails that document a policy, decision, significant action, or how a case was managed
- records that help explain the history of a relationship, [decision](#) or project

## Operational Needs

- data that is needed for ongoing business
- information that is integral to a file about one event, client, or issue (i.e., a case file)
- reference material with ongoing value to the office
- work unit activities documentation ([e.g.](#) work schedules, assignments)

## Official Communications

- formal communication about Commission business
- social media post officially announcing a new Commission program

## Official/Final Records

- final reports and recommendations
- official copies of agendas and minutes
- official copies of policies, directives, procedures, standards, guides
- signed briefing notes



## Recordkeeping systems in the BCER

**Structured shared drives**, (with the *Administrative Records Classification System (ARCS)* and *Operational Records Classification Systems (ORCS)* applied)

Properly configured **SharePoint sites**, with ARCS and ORCS applied

**Line of business applications** (e.g., case management systems such as AMS and IRIS)

**Hardcopy (paper)** filing systems

## Tools



Email clean up tools in Outlook

Assign policy tool in Outlook

A few email principles



# Tools – Managing Email Guide

## Deleting Email Appropriately

Now that you know what constitutes an official email record and how to save them properly, you should delete the redundant (duplicate) emails from your Outlook. You are also encouraged to delete transitory emails, personal emails and other non-record reference material that is taking up valuable space.

Deleting emails quickly and appropriately ensures that your inbox will remain clean and clutter-free.

This section will provide guidance on simple Outlook tools that will help you to delete your emails appropriately. It will also include simple exercises you can perform to find and delete common categories of transitory email.

Tools include:

- **Clean-up Tool**
- **Auto-delete Folders**
- **Assign Policy for transitory emails**
- **Empty Deleted Items on Exit**
- **Exercise: Find and Delete Emails to Distribution Lists**
- **Exercise: Find and Delete Meeting Requests**

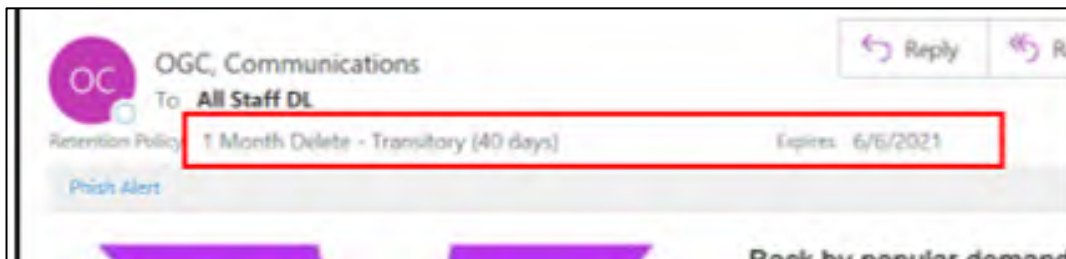
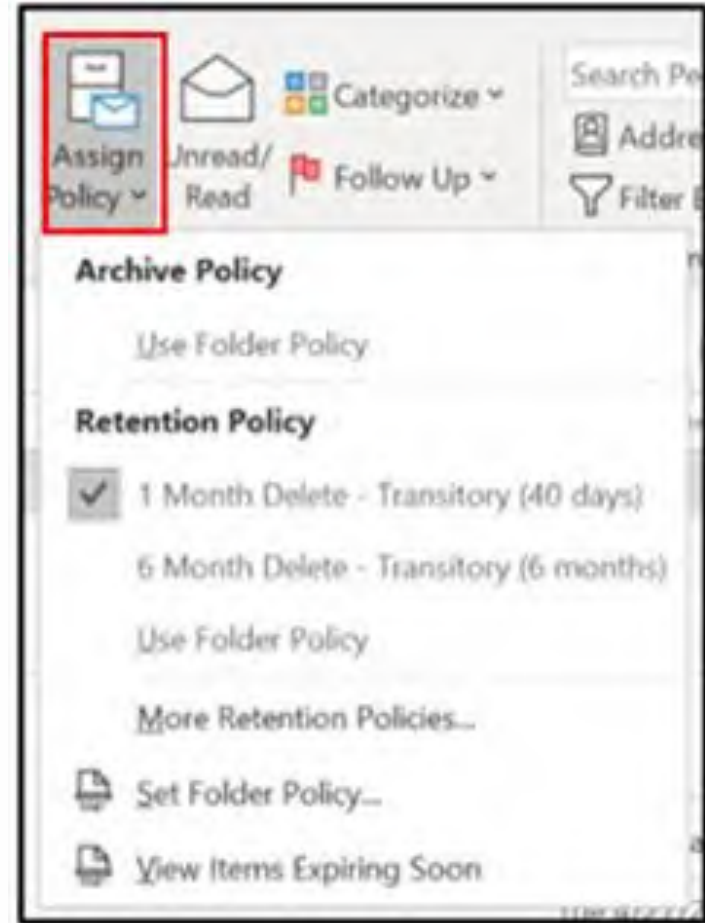
**NOTE:** You are prohibited at all times from 'triple-deleting' emails ([i.e.](#) attempting to purge an email from your 'Recover Deleted Items' folder).

This should not be confused with double deletion, which happens when deleted emails are cleared from the 'Deleted Items' folder. The double deletion process is important for clearing space in your Outlook account but must only be done if the items in question are permitted to be disposed of.

# Assign Policy in Outlook

To apply the policy directly to an email:

1. Select the transitory email and click on the Assign Policy button.
2. Choose the retention you prefer for the email from the picklist.
3. Notice the email now states your chosen retention period, with the “expires” (deletion) date. When the email reaches the expiry date it will be automatically deleted and moved to your Deleted Items folder.



## Governing Principles – Emails.



- The email sender (initiator) is responsible for saving internal email
- The principal receiver is responsible for saving external email
- Working groups should assign responsibility for shared mailboxes

### Bonus good practice tips:

- Empty Deleted Items on exit from Outlook
- Working groups determine who is capturing the official record for a file

# Resources

[Information Management on the Energy Exchange](#)

[Transitory Information Video](#)

[Email Management in an FOI World video](#)

[Documenting Decisions Training video](#)

## Transitory Records

Understanding which records are transitory is one of the key "tools" for information management. Official records need to be kept for specified periods according to legislation and policy. Transitory records, on the other hand, are temporary and low value. They are only needed for a limited time to complete a routine action or prepare a subsequent record (such as a new version). Information is often considered transitory when it does not document decisions or work activities. Each of you has the authority to delete transitory records when your use is complete.

- [Managing Transitory Information Guide - New!](#)
- [Transitory Information Quick Tips - New!](#)
- [Official vs Transitory Records](#)
- [Managing drafts and working materials](#)





# Questions?



## SCRIPT: MODULE ONE, MANAGING EMAIL IN AN FOI WORLD

Hello from your Records & Information Services Branch! Today we are talking about email management in the context of Freedom of Information or, as we more commonly say, the FOI world. Email management is a challenge that we all take different approaches to. Some of today's tips may already be part of your daily habits, but with so much of our business being conducted through email, we thought a refresher would be helpful.

We are focusing on the connection between Freedom of Information and emails because the Commission receives a significant number of FOI requests - an average of 60 a year. Depending on the topic, requests for information can involve many staff and program areas through the Commission, and an FOI request often includes all related email communications.

To begin our conversation about email management, let's review some best practices for emails in an FOI world.

First, remember to keep communications professional, not personal. Emails requested under FOI cannot be altered, so when you write an email always think: would you feel comfortable seeing this in a newspaper article? Would you mind your supervisor or our executive reading this? If in doubt, then don't write it down. . . Remember, "embarrassment" is not an exception to disclosure under the Freedom of Information and Protection of Privacy Act!

Another best practice is to keep your emails limited to one topic. Trying to cover several topics in one email can be a problem for a couple of reasons – first, it can be unclear where to file your email in the recordkeeping system (such as in Kermit, or on the shared drive). Second, it can cause us to provide extra and unnecessary information in response to an FOI request. Unrelated information cannot be removed or redacted from a record unless one of the sections of the Act applies. Just because the information doesn't relate to the topic doesn't mean it's automatically out of scope. Limiting your email to one topic makes it easier to manage as a record, and supports a 'tidier' response for FOI.

So, now that we're creating great email communications... how can we make searching for them in Outlook easier? Well first, know what you can get rid of on a daily basis – what we call your transitory material. Also know what is non-transitory and needs to be kept as an official record, to document or support the work you are conducting for the Commission.

Transitory records are records of temporary usefulness – they're only needed for a limited period of time to complete an action, or to prepare a final record.

The most common email examples are personal messages, announcements of social events, meeting arrangements, and copies received for convenience or reference – unless you are the person responsible for that matter!

Another transitory email is an email that is part of a "string". When you are having a back and forth email conversation, the **final** email, which contains *all* of the back and forth emails, is the official record

of the conversation, and all of the emails leading up to that can be considered transitory, and deleted from your Outlook.

Another example is if you have filed the email into the recordkeeping system, such as in AMS or KERMIT, the email left in your Outlook is now considered redundant. It's a duplicate, and can be deleted.

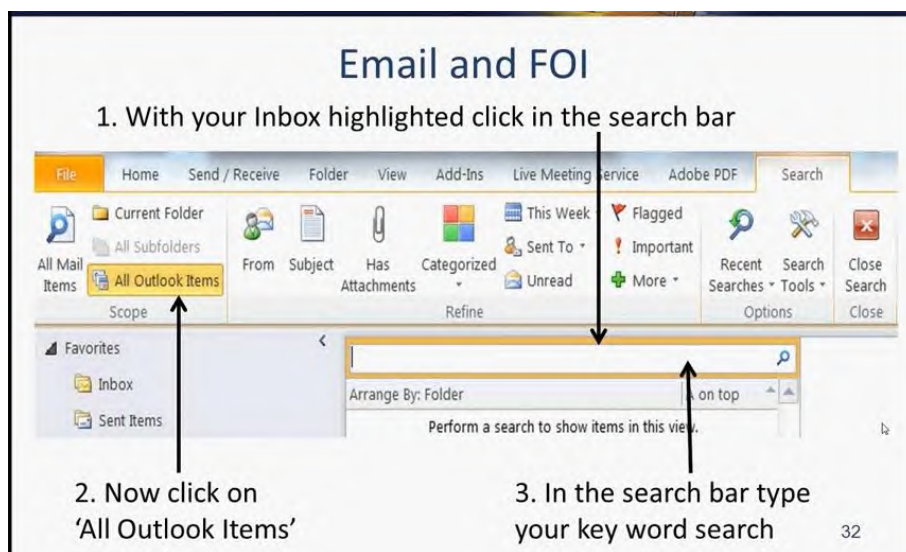
The value of knowing what is transitory is that you can delete those emails when you are done with them. By doing so, you keep your Outlook more manageable, and you're not having to sift through unnecessary records. You can find what you need faster, and easier. It also prevents transitory emails from being included in FOI requests... remember that a request for emails under FOI isn't just limited to the emails in your inbox. It includes your sent items, your deleted items, and anything in your sub-folders.

To end this module, I'd like to share a final tip to help you find all of the relevant emails in Outlook when doing an FOI search (or a search for emails under litigation). If you conduct your search in the order as follows, you should get complete results – this is what's known in the FOI and litigation worlds as 'adequacy of search' and it's what we are aiming for!

First, with your inbox highlighted, click in the search bar.

Now, click on 'All Outlook Items'.

Then, in the search bar, type your key word search.



Today we've covered some key information about email in the context of FOI requests. To summarize, there are a few things we can do to make email management and the FOI search process a little easier:

1. Keep your Outlook tidy – delete transitory items promptly

2. Keep emails to a single topic, and professional
3. Know your proper search methods

We have guides for email management and understanding what is a transitory record on our new intranet section on MyOGC, so please check those out for more information. Thank you and stay tuned for more informational videos!



Hello everyone, in this video I'd like to talk about transitory records - how to recognize them, and how to manage them.

As you may know, we have a few "rules" when it comes to managing Commission records. Official records need to be kept for specified periods according to legislation and policy. Transitory records, on the other hand, are records of temporary usefulness that we only need to keep for a limited period to complete a routine action or prepare a final record (*word bubbles saying "notes that are transcribed into a system" "do you have time to meet today?" "draft # 3, grammar fixes"*). The basic principle is information is considered transitory when it does not document decisions or work activities.

Who can decide if a record fits the transitory criteria? You can! Using your good judgement, when you are finished using the record, you can simply destroy it.

### **First, how do we recognize a transitory record?**

We will start with the obvious categories, such as announcements of social events, personal messages or advertising material.

Then there are transitory records of short-term use, such as:

- Copies created for convenience or reference.
- Duplicates, partial copies or extracts, which you are no longer referencing.
- Input source documents, which are no longer required because the information from them is in the official system.
- Meeting arrangements.
- A simple message saying something like "can you call me this afternoon".
- And Cc copies on emails— unless you are the key staff member for that matter.

Finally, there are records related to drafts and working materials. Drafts, and routine correspondence about revisions, can be transitory. Working materials, such as outlines, calculations, preliminary notes and other rough content that you use to prepare a final record, can be transitory. However, if a draft, email, or other record is essential to understanding Commission business, such as how you reached a particular decision, then the record is not transitory and must be kept. Working materials relating to the preparation of legislation, regulation, or audit reports must also be kept. Outside of these, you can discard those seven versions that provide no information on decisions or approvals once you have a complete and final document.

Each Commission employee has the authority to identify a transitory record, so **you** can determine whether a record is, or is not, transitory.

**So, how do we manage transitory records?**

By promptly destroying them. This helps us to better identify and file official records into our recordkeeping systems, where we can find them more easily. It keeps our email accounts clear of unnecessary clutter. The Commission avoids unnecessary costs for storing and processing transitory records, and it supports the Freedom of Information, or 'FOI', process (*see our video "Email Management in an FOI World" for more information on that!*).

There is one important exception related to destroying transitory records - if we receive an FOI or litigation search request, we must provide all relevant records, including any transitory information that exists at the time of the request. Transitory information that is subject to such requests must be held pending completion of the applicable FOI response process and review period or the applicable litigation activities. (*word bubble: "Do NOT destroy any transitory information relevant to a FOIPPA request or legal discovery!"*)

So now you know how to identify transitory records, and how to manage them. We have some great reference guides on MyOGC such as "official vs. transitory records", "email decision diagrams", and "managing drafts and working materials". And as always, get in touch with your friendly records folks for more information.

Thanks for your time!



# Practical Guidance for the BC Energy Regulator’s Board of Directors

## Legislative Requirements relating to Board Communications (Email) and Records

### Introduction

---

The Regulator is an open and transparent crown corporation that is subject to legislative requirements relating to information access and records. As an agent of government, the Board and each Director are governed by applicable policies, directives and legislation relating to the public’s right of access to information under BC’s [Freedom of Information and Protection of Privacy Act](#) (FIPPA) and the retention of non-transitory records (i.e., records of decisions) pursuant to the [Information Management Act](#) (IMA) and the duty to document key activities and decisions.

In the course of their Board-related duties, Directors may exchange communications and documents (records) with other Directors, employees of the Regulator, and third parties using personal email accounts. Such exchanges of information fall under the control of the Regulator making them subject to FIPPA and the IMA, so it is important to manage these records appropriately. The following information has been prepared to support Directors in understanding and meeting their legislated responsibilities in relation to these Acts.

### Records and Information Management

---

#### Definitions:

Term	Description
Government record	All recorded information created or received by government bodies while conducting business activities and maintained as evidence of those activities, regardless of their digital or physical format. Under the <a href="#">Interpretation Act</a> , a record includes “books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise.”
Transitory records	Records of temporary usefulness that are not required to support or document the Regulator’s business or decision-making activities. As with all records, they can exist in any format or medium (e.g., paper or electronic). Transitory records can be deleted or destroyed when no longer needed for reference purposes.  Examples of transitory records include:

	<ul style="list-style-type: none"> <li>❑ Emails, correspondence and attachments that do not document a business activity or decision (i.e., message content lacks substance).</li> <li>❑ Drafts of documents with no significant annotations, comments, approvals, or substantial changes.</li> <li>❑ Reference copies (e.g., for meetings) not needed as evidence of decisions, actions, or consultation.</li> <li>❑ Rough notes and working materials.</li> <li>❑ Published or unsolicited information from external sources (e.g., advertisements, newspapers, magazines, spam, junk mail, unsolicited correspondence not used for any business decisions or actions).</li> </ul> <p>IMPORTANT: Transitory records cannot be destroyed if an FOI request has been received or eDiscovery initiated, and the records relate to the topic or specified date range.</p>
Non-transitory (Official) records	<p>It is important to understand which records are not transitory. Non-transitory (official) records need to be filed in an appropriate recordkeeping system (e.g., a secure system maintained by the BCER's Corporate Governance branch). If any of the criteria below applies to a record, the information is NOT transitory and should be kept:</p> <ul style="list-style-type: none"> <li>❑ Record supports or provides evidence of a key decision (i.e., of the Board)</li> <li>❑ Record is required to meet legal or financial obligations</li> <li>❑ Record is needed to sustain the Regulator's operations, programs or administration</li> <li>❑ Record is integral to a case (i.e., needed as context for related records in a case file)</li> <li>❑ Record is needed for accountability purposes</li> </ul>
Custody (of a record)	<p>Having physical possession of a record, even if a public body does not necessarily have responsibility for the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing and providing security.</p>
Control (of a record)	<p>Having the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure.</p>

## Director Responsibilities under the IMA:

### Use of Personal Email

- Directors use personal email accounts to exchange information with other board members, employees of the Regulator or third parties.
- Emails related to the business of the Regulator's Board should be kept separate from other types of communications; it may be helpful to:
  - ❑ save them in a separate folder; and
  - ❑ include a standardized subject line in emails to make them easily identifiable and searchable (e.g., **BCER: Q2 Financial Statements**).
- Transitory emails should be routinely deleted when no longer required for reference. This should include deleting them from both the "inbox" and "deleted items" (trash) folders.
- Transitory records that have not been deleted could be subject to an FOI request or eDiscovery. These records cannot be legally destroyed if an FOI request has been received or eDiscovery initiated and the transitory records relate to the requested information.

## Duty to Document

- The Regulator must follow government’s “duty to document” [directive](#) and maintain adequate records of decisions which includes Board records. Refer to government’s video on [Documenting Government Decisions](#) for more information about this requirement.
- The Board Secretary maintains official records of the Board on behalf of the Regulator.
- If a Director creates or receives a communication (e.g. from another Director or third party) that supports board business or provides evidence of board decision-making, a copy of the email and any attachments should be forwarded to the Board Secretary for filing as such records are not in the Regulator’s custody (and thereby inaccessible) but are under its “control”.

## Access to Information / Freedom of Information

---

### **Definitions:**

Term	Description
Freedom of Information (FOI) Request	An FOI request is a formal process to ask for information that falls under the custody or control of a provincial public body. A request must be made in writing and typically relates to specific information held by a public body about an individual (their personal information) or pertaining to its business activities and mandate.
Exceptions to Disclosure	FIPPA establishes an applicant’s right to access records held by a public body, however there are certain exceptions to accessing records. Not all requested information is deemed appropriate for public release. Some exceptions to disclosure are mandatory (information that meets the criteria must be protected), while others are applied to requested information at a public body’s discretion.

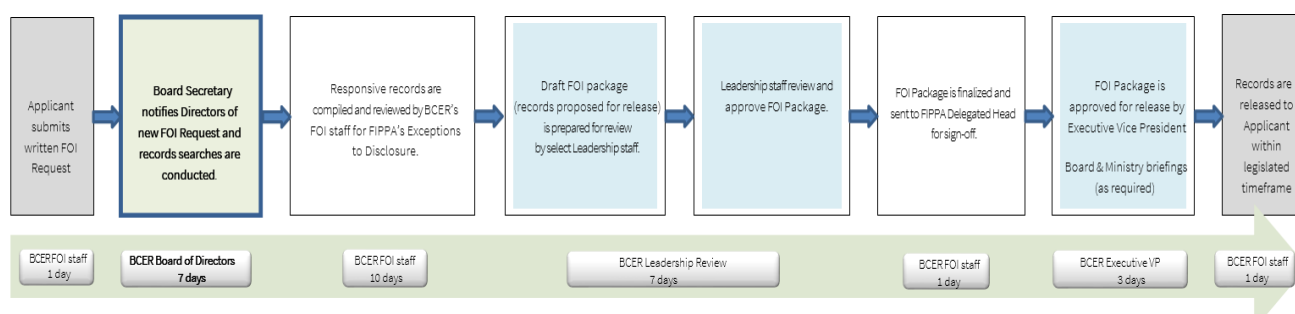
### **Director Responsibilities under FIPPA:**

#### Responding to an FOI Request

- FOI requests typically follow a 30-business day processing timeline.
- When the Regulator receives an FOI request, a formal process is followed:
  1. The first step involves interpretation of the request (i.e., understanding what information an applicant is seeking) and identifying all locations where responsive records may reside.
  2. If responsive records could reasonably include communications held by Directors in their personal email accounts, the Board Secretary will send a “Call for Records” to each Director on behalf of the Regulator’s FOI staff.
  3. The Call for Records is an email that includes the wording of the request, the applicant “type” (e.g., media, law firm, etc.) and any pertinent details to support the search for records.
  4. Directors will be requested to provide the Board Secretary with copies of records, should they exist, that they believe may be responsive to the request.

- An FOI request does not automatically result in the release of information; a line-by-line review of each responsive record in an FOI package is completed by the Regulator’s FOI staff to identify information that should be fully or partially withheld (protected) under FIPPA’s exceptions to disclosure.
- Prior to any release of information, FOI packages are reviewed by select members of the Leadership group.
- Once all Leadership feedback and approvals have been received, an FOI package is signed off by the Executive Vice President, People, Strategy & Transformation (FIPPA Delegated Head); the Board may be briefed on a request as appropriate.
- Records are then released to the applicant within the legislated timeframe for response.

### FOI Request Process Flowchart



### FIPPA’s Exceptions to Disclosure

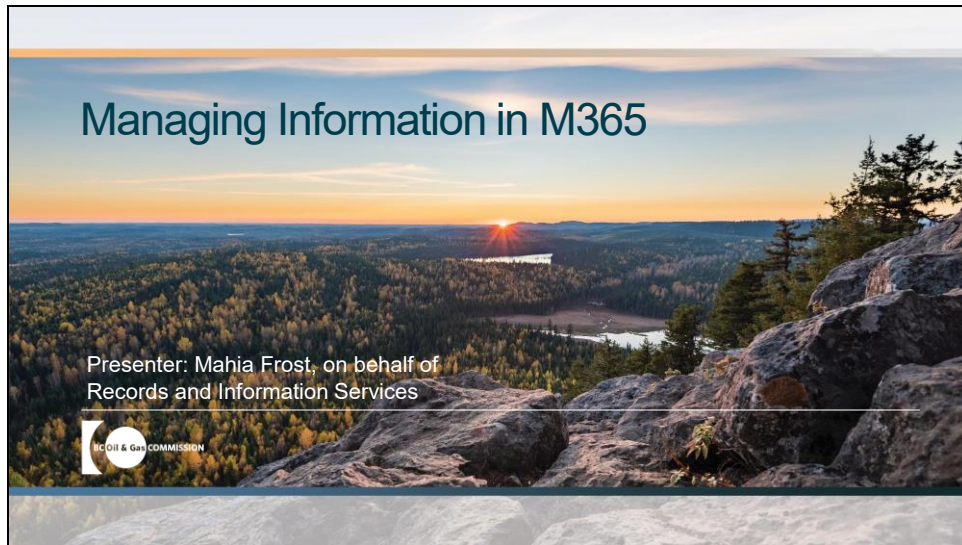
Section	FIPPA Section Title	Description of Exceptions to Disclosure	Application
12	Disclosure Harmful to Cabinet Confidences	Information that would reveal Cabinet confidences (e.g., advice, recommendations, policy considerations, legislation or regulations submitted or prepared for submission).	Mandatory
13	Disclosure Harmful to Policy Advice, Recommendations or Draft Regulations	Information that would reveal advice or recommendations. This section is intended to allow for full and frank discussion of policy issues during deliberative processes.	Discretionary
14	Disclosure Harmful to Legal Advice	Communications between a public body and its legal counsel to protect solicitor-client privilege.	Discretionary
15	Disclosure Harmful to Law Enforcement	Information that could harm a law enforcement matter.	Discretionary
16	Disclosure Harmful to Intergovernmental Relations or Negotiations	Covers matters that could harm the relations between BC levels of government and governments from other provinces and jurisdictions (e.g., Government of Canada, council of municipality, regional district board, aboriginal government, government of a foreign state, international organization of states).	Discretionary
17	Disclosure Harmful to Financial or Economic Harm	Information which could cause financial or economic harm to a public body or to the government.	Discretionary

18	Disclosure Harmful to Conservation of Heritage Sites	Information about heritage sites which would result in the exploitation or destruction of those sites.	Discretionary
18.1	Disclosure Harmful to Interests of an Indigenous People	Information that could reasonably be expected to harm the rights of an Indigenous People to maintain, control, protect or develop their cultural heritage, traditional knowledge, traditional cultural expressions, or manifestations of sciences, technologies, or cultures.	Mandatory
19	Disclosure Harmful to Individual or Public Safety	Information that could result in harm to any person's mental, physical, or emotional health or to public safety.	Discretionary
20	Information that will be Published or Released within 60 Days	A public body may withhold information from an applicant if it is already for sale to the public, or if the public body plans to release or publish the information within 60 days.	Discretionary
21	Disclosure Harmful to Third Party Business Interests	Public bodies are often in possession of commercial or financial information related to outside businesses and must withhold that information from an applicant if release would cause harm to the business. A three-part test must be met for a public body to appropriately apply section 21.	Mandatory
22	Disclosure Harmful to Personal Privacy	Personally identifiable information must be protected. Except in limited circumstances, a public body must not release an individual's personal information without their explicit consent.	Mandatory

## Additional Resources (available soon on the Board Portal)

---

- Video: Transitory Records
- Video: Email Management in an FOI World



Hello, and welcome.

My name is Mahia Frost, and I am presenting on behalf of the Records and Information Services Branch. We are the team that supports Commission staff on how to manage our information according to best practice and legislation.

I would to acknowledge that we are honoured to be living and working on the traditional territory of the Lekwangan speaking people.

Today we are going to talk about managing information in the new technological environment, Microsoft 365.



**New Tools**

We have new tools that we use to work together, collaborate, and share information.


Today we focus on making sure you know what our requirements are for working in these spaces.

**The Same Rules**

2

Why are we here? Microsoft offers new tools and new ways to access and use our information. Has this changed the rules for how we manage our information? No!

This session will cover the rules and the tools.

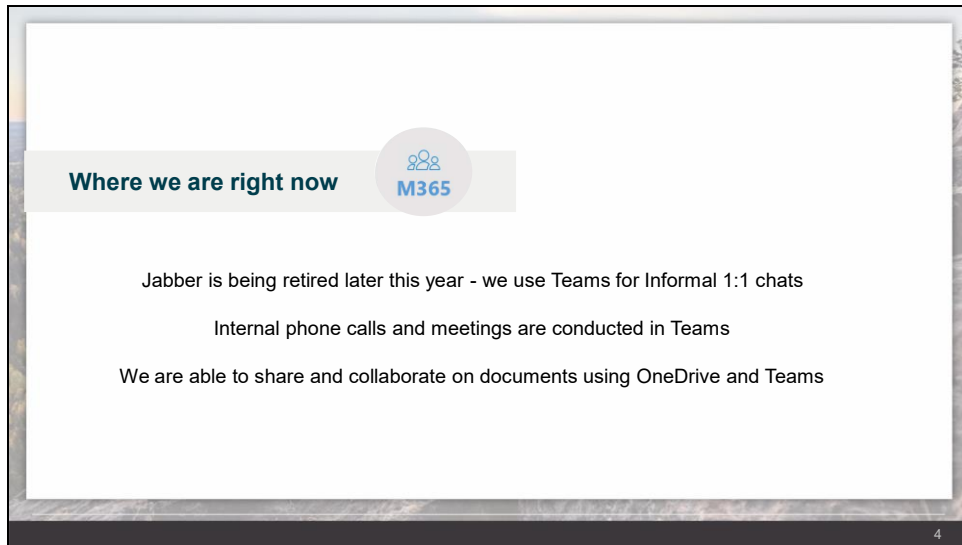
**Learning Objectives** 

- Understand the intended use for each workspace
- Understand our collective and individual responsibilities
- Understand what is a transitory record and how to manage them
- Know where to find the guidelines on web pages

3

Our learning objectives are quite simple:

We want you to understand how we will use these new 365 workspaces, our responsibilities for managing information in them, what we mean when we say transitory records, because you will hear us talk a lot about this when we talk about 365, and how to find resources in the future.



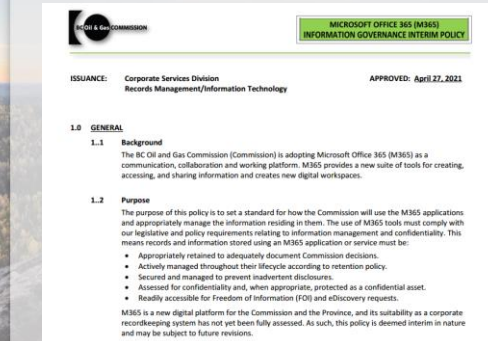
Office 365 is the new normal in the Commission and government.

Currently at the Commission we are primarily using the Teams application for conducting meetings, chatting, and supporting internal phone calls.

To support this technology, Records and IT developed a policy to provide a framework for how we use these tools.

## M365 Information Governance Interim Policy

This policy guides us on how we should manage information in 365.



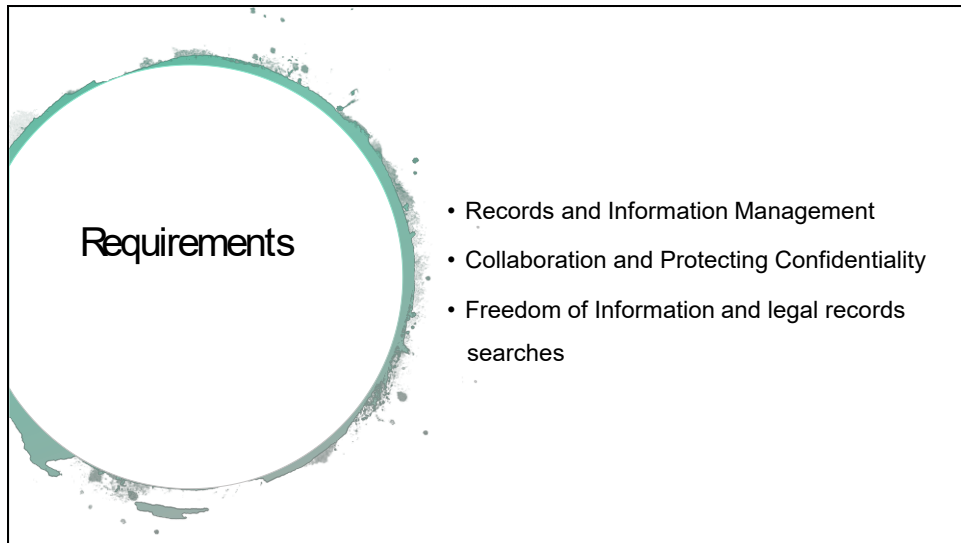
5

We have called it the M365 Information Governance Interim Policy.

Information Governance is the overall strategy for managing information in an organization. This policy tells us how we should manage information in 365.

It is an Interim policy because we are in a learning curve. This is a new platform for all of us, and we expect that there will be changes as we become more familiar with how we use these tools and what they offer. We are also assessing whether it will be appropriate for managing our electronic records over the long term which will affect the final policy.

We shaped this presentation to the structure of the policy. It's important we all understand our collective and individual responsibilities.



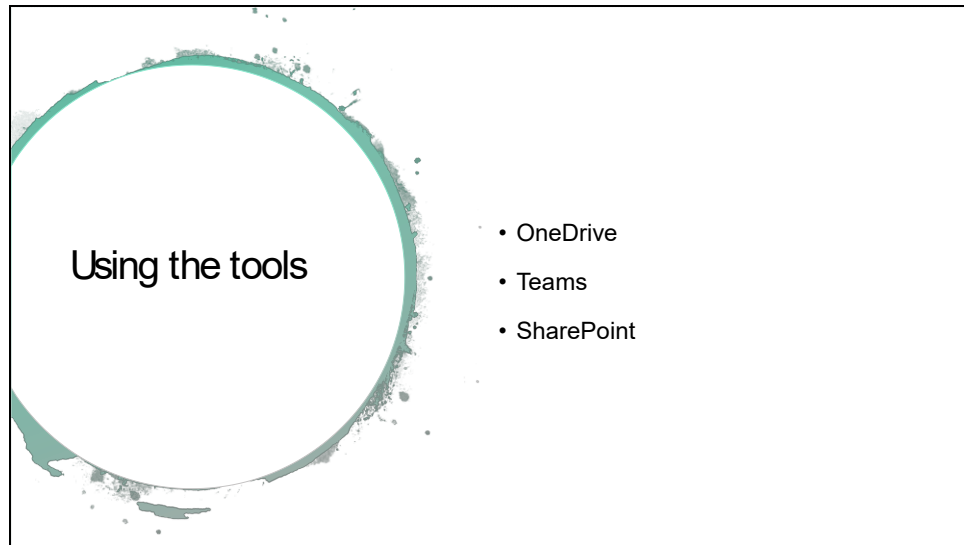
So here are the rules. The first part of the policy covers the requirements which apply to all of us. It is broken out into these elements.

First is records management: official records within 365 workspaces must be saved to an appropriate recordkeeping system, which is usually our shared drives, to ensure Commission decisions are adequately documented and business continuity and operations are supported.

The Collaboration and Protecting Confidentiality section says that users must limit the sharing of sensitive or confidential information, (such as personal information), and outlines what that looks like in 365.

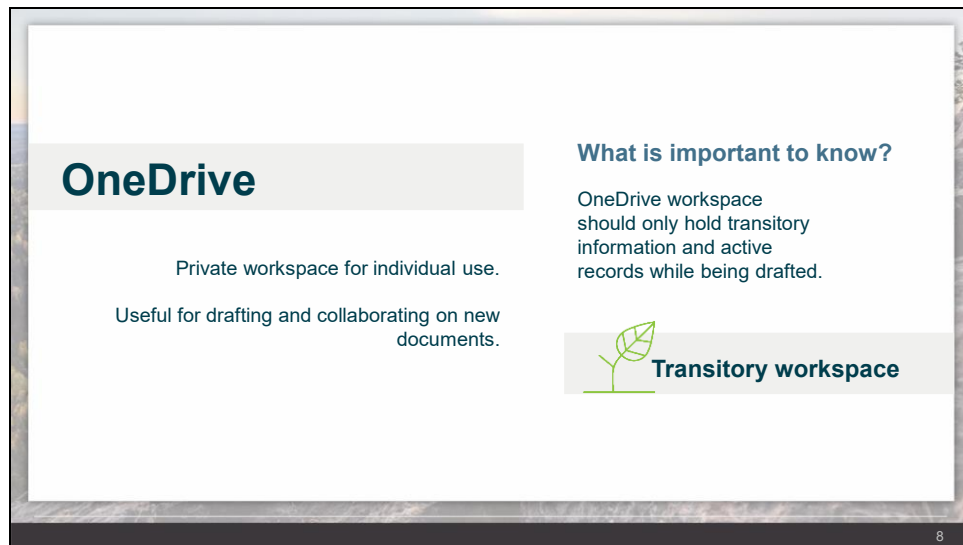
Information in M365, like all Commission information, is subject to the Freedom of Information and Protection of Privacy Act (FOIPPA) or other legal obligations, and we must be prepared to search for and gather records that are responsive to these types of requests.

To summarize, you have to save your records to the shared drives, protect confidentiality, and remember that all areas of 365 are subject to FOI or legal searches.



The policy then moves to more of what this means to us. It's broken out into application specific sections – meaning OneDrive, Teams, and SharePoint.

First let's talk about OneDrive.



OneDrive is both a platform for sharing documents for collaboration, and to hold transitory information that is useful to you. Like your F: Drive, you are the only person who has access to the records in this space, unless you specifically share something. Because of this, it is not an appropriate place to hold official records for the Commission, such as original records relating to your work.

**Let's talk a little more about why we don't use OneDrive for official records:**

- You are the only person who sees your OneDrive contents, but your OneDrive content is subject to FOI and legal records searches.
- If you keep official records in OneDrive, they are not accessible by others who may need access to them, and
- We have no way of appropriately managing the records.
- We call these "information silo's" and we want to avoid that.

**So, what DO you use OneDrive for?**

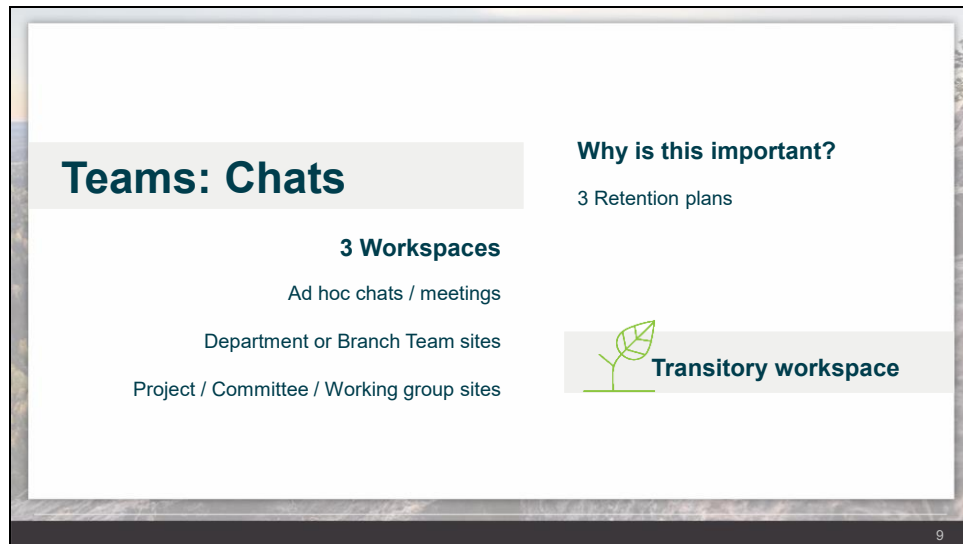
- Working material that you are not ready to share with your team yet
- Sharing a document with select people for collaboration.
- Transitory drafts, and convenience copies
- Personal reference material

You may keep some copies of documents for quick reference, or drafts of documents – but once you have a final version of that draft, or even if it is stalled but might be picked up in a year – it's important to move it out to the shared drive so it becomes part of the record for that activity.

Supervisors may opt to keep a copy of personnel records in their F: Drive or their OneDrive. This may be a copy of their staff's IDP's, or vacation requests. The official records of these are with HR, but we understand the desire to have that information at your fingertips... Since what you have is a copy, kept for convenience, OneDrive is an acceptable use for that. It keeps it secure and accessible to you.

Just remember that Commission records should be filed in our shared drives. When you are finished working on that document in OneDrive, move the final over to your shared drive.

Now let's talk about Teams.



Teams is probably our most used application for M365 so far, and the policy dictates both how we use it and how long we keep the chat data within it. We have all started using Teams for meetings and chats.

You may have also noticed that IT is rolling out Teams sites. There are two types of Teams sites – Teams built specifically for each branch or department, and Teams for specific working groups, committees, or projects. The intended use for each site determines how long we keep the information in it.

It is important to understand that Teams is not an appropriate recordkeeping system. Teams is for transitory communication. This is key. We don't want to hold official records within this workspace.

With that as our basic principle, we manage Teams chat data in three ways:

- One-on-one chat messages are automatically deleted after 10 days, and this is fine, because we are only using this for transitory purposes.
- Department/branch chats (within a Teams Site) are automatically deleted after three months. This includes both private channels and branch channel chats.
- Project/committee/working group conversations (within Teams Sites) are kept for the duration of the project, then deleted at the end of the project, after the lead has confirmed that any official records within the site have been pulled or copied out.

This is important for you to know because it gives you timelines for capturing official information out of Teams.

Most of you will have attended a Documenting Commission Decisions workshop, and those principles apply here. Any official or critical information in Teams must be captured in the recordkeeping system, this includes context for a business decision, or a record of a decision. This means that if your chat conversation has strayed into decision making territory, you will want to summarize or copy it out before the 10 days has lapsed.




**Teams: Documents**

Uploaded or shared documents for collaboration

Information sharing

**Why is this important?**

Official (altered) records need to be moved and saved to the recordkeeping system.

 **Transitory workspace**

10

The chat retentions we just talked about do not apply to documents in Teams. This means that documents are not auto-deleted the way chats are – uploaded documents reside in a team site until the Teams site is closed. It also means that we have to manage them more actively.

As you may have figured out, there are a few ways to share documents in Teams, and that is a whole other conversation. Our focus is on what you do with the documents once you are finished with them. As we have said, Teams is transitory workspace, so if you have created or completed a document in this space, it's important to remember to move it out to the recordkeeping system.

For example, if you use Teams for collaboration on a document, make sure one of you takes that final version of the document, and puts it into the appropriate folder on the K: Drive. If it is sitting outside of a Teams site, in a 1:1 chat, you won't see that document after 10 days, so make sure you stay on top of this.

Let's talk about Transitory Records since we have referred to them so many times.

**Transitory Records**

Not all commission information is of long-term value and needs to be retained.

- Drafts
- Convenience
- Rough notes
- Unofficial Copies
- Meeting arrangements
- Working material
- Input documents
- Messages

11

The phrase we keep using – TRANSITORY RECORDS. Per legislation, all recorded information is a “record”, and needs to be managed according to retention schedules. This means that our Teams chats, our Word documents, all the things we are creating and receiving are records, but there are different categories of records. All records need to be managed according to approved information schedules (i.e., ARCS/ORCS/Transitory Schedule).

Transitory information is information of temporary and/or low value that is only needed for a limited period of time in order to complete a routine action or prepare a subsequent record (such as a new version). Each of you has the authority to delete transitory records when your use is complete.

So, these may be rough notes and working materials. **Context** and **content** help determine whether a record is transitory. For example, preliminary notes relating to planning a training session are more likely to be transitory than notes relating to drafting regulations or establishing a new commission program.

Other transitory records:

- Copies kept for convenience and quick access
- Printed out agendas for meetings (not that we are doing that these days!)


It's fairly common sense, but let's break it down a bit more.

## Messages / Communications

### Transitory

- announcements of social events
- cc copies (unless you are the main staff member responsible for the matter)
- meeting arrangements
- routine correspondence about drafts and revisions
- requests to call someone
- emails conveying an attachment (e.g., "please see attached", and after the attachment is saved)

Messages or attachments that are required to support ongoing business needs.



### Not transitory

12

Messages can take many forms - email, instant messages such as Teams chats, social media postings, or voice/video message recordings. Transitory messages are messages of only passing value that do not support or document a business activity or decision. We have examples of transitory messages on the screen, which covers:

- Emails which announce social events, such as our Tuesday Trivia Challenges, or cc copies (unless you are the main commission member responsible for the matter, because then you hold the official record)
- Meeting arrangements
- Routine correspondence about drafts and revisions
- Requests to call someone, and
- Emails conveying an attachment, once the attached record is saved

Messages that are required to support our business needs are **not transitory** information. Due to their content, or the context they provide, they must be retained (such as an email documenting a policy decision or advice, chat agreeing to a course of action, or social media post that is the initial announcement of a new program).

Just a housekeeping note: once these "not transitory records" have been saved into the right folder on the K: Drive any copies of the messages may be considered transitory and deleted. For example, once you have copied an email to a folder on the shared drive (your recordkeeping system), you can delete the original in Outlook. It is a good practice, because if you leave it in Outlook, it may cause confusion down the road to whether you have filed it or not.

Let's talk about transitory drafts.

**Drafts**

**Transitory**

**Typical features of transitory drafts:**

- Incomplete
- Are not documentation of decisions, approvals, or substantial revisions
- Interim drafts that reflect minor editorial changes
- Superseded by a subsequent draft/final version

**Typical features of non-transitory drafts, which should be retained in your recordkeeping system:**

- Complete
- Intended for consultation and review
- Document decisions, changes, and approvals

**Not transitory**

13

**Transitory drafts** are incomplete versions of a document which have been superseded by a new version. They will typically contain minor edits. Once a subsequent draft or finished record has been developed and filed, transitory drafts are no longer needed.

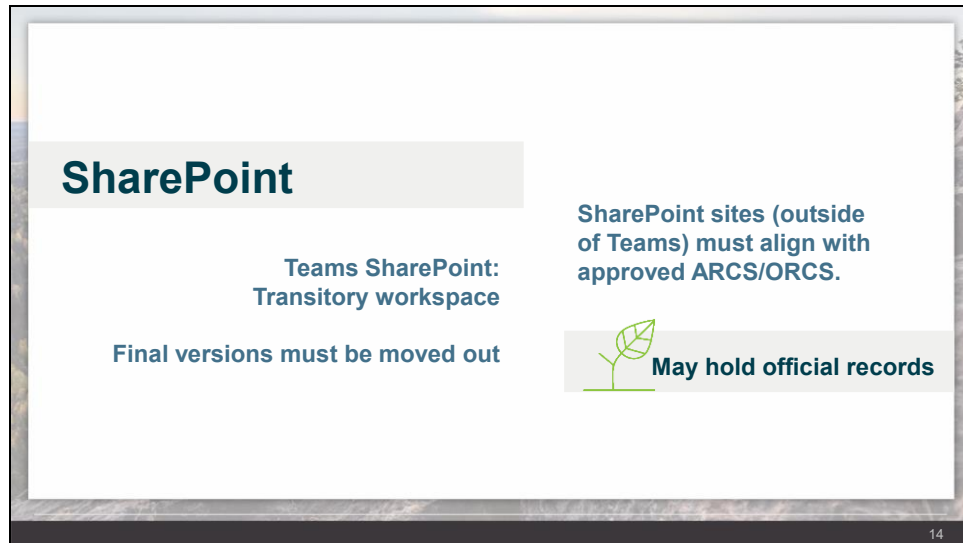
On the other hand, a draft which document decisions, has substantial changes, or approvals is not transitory. Consultation versions with input from stakeholders are not transitory. These should be retained. Draft legislation, audit reports, and other significant drafts are **not** transitory.

And of course, we must never destroy any transitory information that may be relevant to a current/anticipated *FO/PPA* request or legal discovery.

This concludes the transitory records part of the training.

We want to make sure everyone understands this because it helps clarify what we mean when we say a workspace, such as OneDrive, or Teams should only hold transitory information in the longer term. And if you do have official information, it should be moved to the recordkeeping system on the shared drive. This ensures that the records are preserved, managed, and easily found for future use.

Back to the last 365 tool we are going to talk about – SharePoint!



The policy also addresses SharePoint. There are two main uses of SharePoint in 365, SharePoint inside of Teams and SharePoint outside of Teams. As you get your Teams sites for your branches and projects, you will notice that it uses SharePoint as the platform for sharing and collaborating on documents. Each Teams SharePoint is specific only to that Team and intended for short-term use and collaborative purposes, not for storing records.

**SharePoint in Teams** is a transitory workspace. Official records created within this workspace must be moved out of the Teams environment and saved to the recordkeeping system on your shared drives.

**SharePoint sites outside of Teams** are typically used as broader communication tools or collaboration hubs at a corporate level. These SharePoint sites are retained for a longer duration, and content must be managed according to records lifecycles and retention rules. Site structure must align with approved information schedule classifications. Our branch will be working with you, and IT, when these sites are developed to ensure we put the right foundations in place.

You have learned a lot today... so let's end this by showing you where you can find resources for future reference.

MyOGC  
Resources

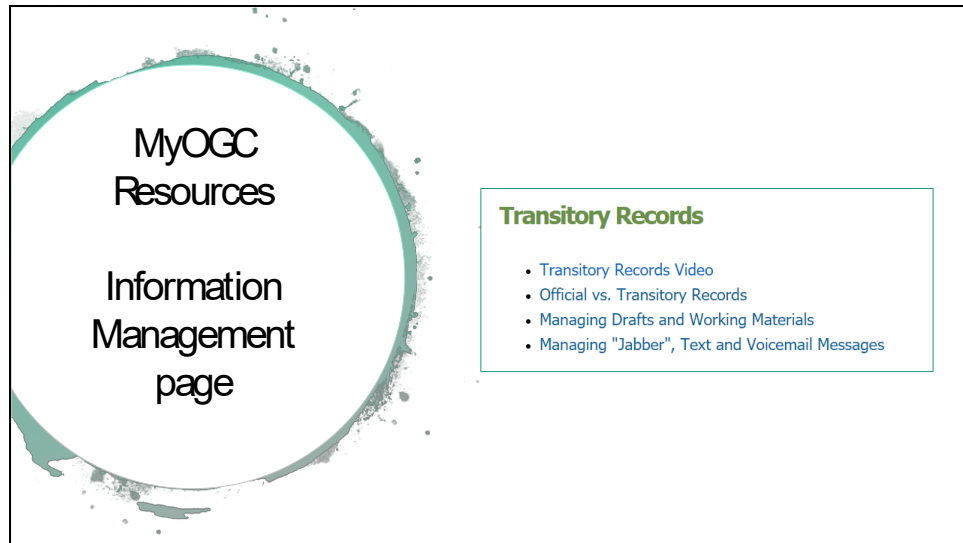
M365  
Information  
and Training

Resources / Tools

- [Teams Quick Start Guide](#)
- [Quick Start Teams Video](#)
- [Teams Cheat Sheet](#)
- [Teams FAQs](#)
- [How to Share a Document in Teams](#)
- [How to Save Teams Chats into Shared Drive](#)
- [How to Save Documents from Teams into the Shared Drive](#)
- [How to Save a Teams Meeting recording into Shared Drive](#)
- [Teams BCOGC Records Management Guide](#)

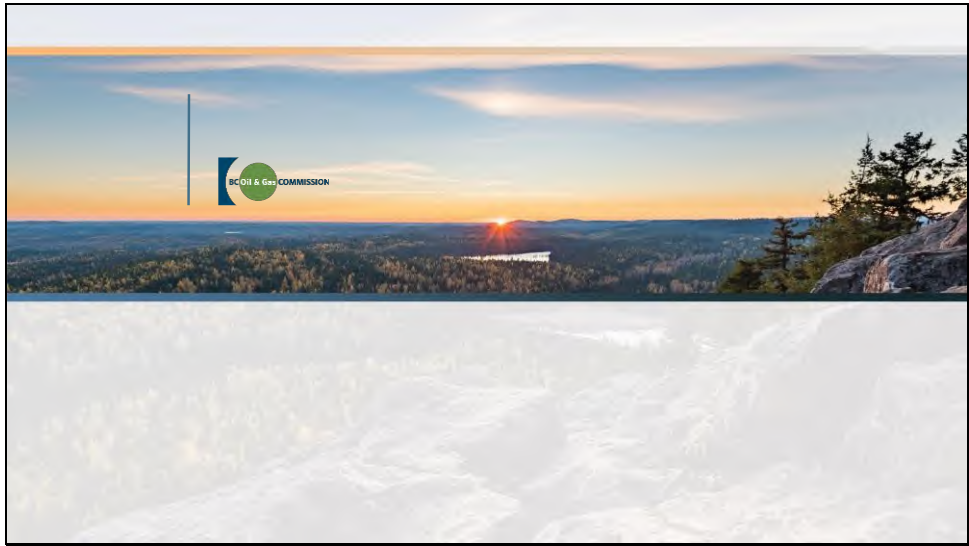
There are a wide range of M365 guidelines that have been created by your IT and records teams. They are on the [M365 information and training page](#), under the Technology tab of MyOGC. For example, in the Teams section, which we show here, you will see How-To guides related to [saving Teams chats into the shared drive](#), [saving documents](#), [general records management guides](#), etc.

Check them out if you have questions.



As a final slide, we want to point out additional guidance related to transitory records. You will find these under the Corporate Tab, on the [Information Management page](#). We encourage you to use these resources.

Thank you for your time! As a reminder, our branch is always available to help you and answer questions.







# Shared Drive Organization

in the BCER





# 3 Goals



# 3 Goals

1. De-duplicate
2. Shorten long file paths

 > This PC > shares (\\bcogc) (K:) > RIM Victoria > LAN organization projects 432-60

3. All folders clearly relate to an ARCS/ORCS classification



# Information Schedules:

## **ARCS = Administrative Records Classification System**

*Covers: committees,  
human resources,  
financial management,  
agreements  
IT projects,  
etc...*

## **ORCS = Operational Records Classification System**

*Covers operational BCER work which supports our mandate*

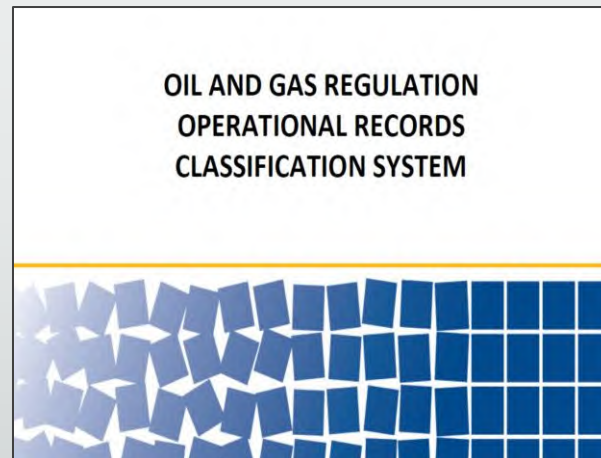


# Information Schedules:

ARCS = Administrative Records Classification System

ORCS = Operational Records Classification System

*Just to be clear... ORCS = this*



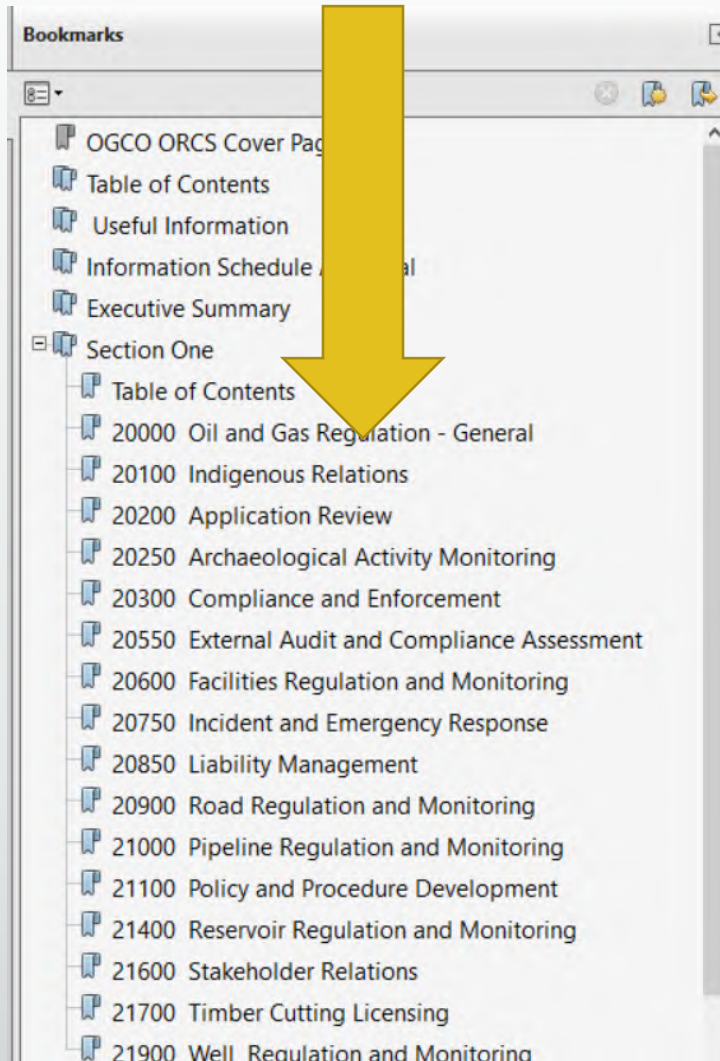
*Not this:*





# OGCO ORCS Primaries

*See how they relate to what we do?*



## OIL AND GAS REGULATION OPERATIONAL RECORDS CLASSIFICATION SYSTEM



**OPERATIONAL RECORDS CLASSIFICATION SYSTEM**

This is an approved information schedule, as defined by the [Information Management Act \(SBC 2016, c. 27\)](#). For more information consult your [Records Officer](#).

ORCS Primary 20900



**20900 ROAD REGULATION AND MONITORING**

Records relating to permits for use of and access to roads as part of the infrastructure required for oil and gas activities such as wells, pipelines, and facilities. All permits are issued in accordance with the *Oil and Gas Road Regulation (B.C. Reg. 56/2013) (OGRR)*, but this primary also covers roads or portions of a road originally authorized and constructed under the *Land Act (RSBC 1996, c. 245)* or the *Petroleum and Natural Gas Act (RSBC 1996, C. 361)*, as a Petroleum Development Road. Authorization for the permit holder to make changes in or about a stream comes from the *Water Sustainability Act (SBC 2104, c. 15)*.

- There are a variety of types of oil and gas roads applicants may apply for, such as:
- Long-term, all-weather roads: roadbeds surfaced with gravel.
  - Short-term, low-grade roads: constructed during non-frozen ground conditions.
  - Snow and/or ice roads: activities carried out during frozen ground conditions with minimal soil disturbance.

The records in this primary document the road "activity file." Road permit holders have obligations regarding the construction, maintenance, use and deactivation of oil and gas roads, including clearing widths, bridges and culverts, hazard warnings and post-construction reporting.

NOTE: The classifications in this primary apply to the official copy of the records, regardless of media, and include data held in systems.

For a list of classifications removed from this primary, see Appendix A: *Summary of Amendments to the OGCO ORCS*.

For inspections, see secondary 21300-50.

For operational policy, see secondary 21100-00.

For road permit applications, see secondary 20200-20.

The agency OPR is the Oil and Gas Commission unless otherwise noted below. See specific secondaries for OPR retention schedules.

	A	SA	FD
All non-OPR offices will retain these records for:	SO	nil	DE
<b>-01 General</b>	CY+1y	nil	DE
<b>-20 Road files</b> (formerly called Petroleum Development Roads (PDR's), this secondary covers the post-approval activity information for road permits, which approve the construction of roads, bridges and culverts for oil and gas activity) (includes maps, special studies, reports and notices, and for original PDR files, the applications)	SO+5y	nil	FR
SO: when the road has been cancelled or deactivated, and restoration is complete	(cont)		

ORCS Secondary -20



The classification number is 20900 -20.

It covers activity records for roads.





# ORCS Secondary

20000	-10	<p><b>Statistical and activity reports</b>          (covers ad hoc, statistical and routine reports that are not part of an operational file, such as a compliance file or well file)</p> <p>SO: when information is no longer required for statistical, reporting, or analysis purposes</p> <p>NOTE: This secondary covers the various reports produced by the Commission, such as weekly/monthly/quarterly reports, which are not classified elsewhere in this ORCS. It does not cover, for example, annual reports, service plans and annual activity reports, which are classified under secondary 21600-20, or technical/data reports for operational activities such as wells or pipelines, which belong on the individual activity file.</p>	SO	nil	DE
-------	-----	---	----	-----	----

Classification number  
20000-10

Retention codes  
which provide the  
management plan for these records



# An ARCS primary

## 102 - Administration, Staff Meetings

[ARCS](#) > [Administration](#)

Records relating to ministry/agency staff meetings, including internal management-level meetings.

Record types include correspondence, agendas, minutes, and reports.

**non-OPR NOTE:** Offices will retain non-OPR copies of records for SO nil DE

Primary- Secondary	Records Series	OPR		
		<i>A</i>	<i>SA</i>	<i>FD</i>
102-00	Policy and procedures	SO	nil	DE
102-01	General	CY+2y	nil	DE
102-20	Staff meetings DE= Staff meeting records can be destroyed upon authorization of the Records Officer because information concerning significant agenda items are included in ministry/agency executive committee meetings, which are selectively retained by the government archives under the Executive Records schedule ( <a href="#">102906</a> )	CY+2y	nil	DE



[Previous](#) | [Next](#)

# Herding Cats



**It CAN be done**



# To-Do List for Shared Drive Projects

- ✓ *Reduce duplication*
- ✓ *Reduce long file paths*
- ✓ *Assess security requirements*
- ✓ *Create good structure*
- ✓ *Move files to new folders as necessary*
- ✓ *Train staff for maintaining structure*



## What it looks like:

- 📁 Audit and review files 975-40
- 📁 Lists spreadsheets and registers 100-05
- 📁 ORCS Development 432-40
- 📁 RM projects and plans 432-60
- 📁 Travel files 1240-20

- 📁 \_Forms & Templates
- 📁 Contract Mgmt 1070-20
- 📁 Financial Reconciliations 920-20
- 📁 MOUs and Agreements 146-45
- 📁 Presentations 324-40
- 📁 Procurement 1070-30
- 📁 Staff Meetings 102-20



*Thanks for watching!*



**Shared Drive Projects script.** (★ means change slide)

Hi! Thank you for taking the time to learn about why we want to organize Shared Drives in the Commission, and what our shared drive projects goals are. ★

Shared Drives are our current record keeping system in the Commission. However, they are not structured for being record keeping systems. Introducing structure to commission drives allows us to *manage* our electronic records rather than store them, and lays the path for our future goal of an EDRMS. ★

We have 3 goals for shared drive projects: ★

1. Remove unnecessary duplication – makes the records easier to manage because the focus will be on the official records, and reduces storage costs ★
2. Shorten long file paths – we have a 250 character limit to file paths, which includes document titles. If we go longer than that, we are at risk of our records not being backed up properly. Naming conventions can help with this. Our aim is to keep it intuitive, but not long. ★
3. Every single folder relates directly to an ARCS / ORCS number.

We have a few “rules” when it comes to managing Commission records. One key rule is that every record that is not transitory must have an ARCS or ORCS classification that applies to it, so you can know how long to keep it and what to do with it when that time is done - delete it, (following our destruction processes), or transfer it to the government archives. ★

This rule is born in legislation, which says that you can only destroy a government record in accordance with an information schedule.

ARCS covers administrative records – the housekeeping and common records that you will find in any government organization. ★

ORCS are the custom-built schedules, covering the records that are unique to your organization from the rest of government. ★

They are structured the same way; they just apply to different types of records. They both provide classification numbers for arranging your records, and retention periods, which tell you what the lifecycle is for managing your records.

Next we are going to go through a quick primer to ARCS and ORCS. We are just going to touch on what you will need to understand decisions we make during this project. ★

A building block to ARCS and ORCS are primaries. Primaries are based on a function – what you are doing. This may be negotiating agreements (in ARCS), or doing compliance work (in ORCS). ★

Primaries have a primary number, which is the first part of your classification number, and a title, which describes the function. ★

Within each primary are secondary categories, each one for records that supports the primary function. A secondary has a two-digit number assigned to it, and that is the second part of your file number. ★

A secondary also has a retention period, which lays out management plan for the records. The retention period is broken into a three-stage lifecycle, and uses simple codes, to be system friendly. ★

There is a guide at the beginning of our ORCS, to help interpret the codes. We call the guide “useful information” ★

As we said, ARCS and ORCS are structured the same way – they just look slightly different from each other. This is an ARCS primary.

These are the documents we talk about when we say we are “mapping” your folders to ARCS/ORCS, and these are the classification numbers you will see in your newly structured shared drive. ★

So what does a shared drive project look like? ★


RIS does analysis on your folders, creating a duplicate report and a long file path report. We work with you to start cleaning those areas up. ★

Then we start to create the structure. We talk with you to find out what security permissions need to be applied. We may talk about naming conventions if that makes sense for your team. Our goal is for the structure to work for you. ★

When we set up the structure, and assign the classification numbers to the folders on your shared drive it will look something like this. ★

As we work in your project, we can explain details, but we hope this high level description makes it clear what our aim is, and why are we doing this. We look forward to working with you! ★





# Organizing Shared Drives in the Commission

## A guide for the DIY folks

Records and Information Services  
2020

# Table of Contents

Background: why we are doing this	2
3 Goals for a Shared Drive project	3
Commission Shared Drive principles	3
Getting started	4
Key elements to a successful shared drive project	4
Steps to organizing a shared drive	4
What does this look like?	6

## BACKGROUND: WHY WE ARE DOING THIS

We are building a strong and compliant Information Management (IM) program in the Commission. One of our key goals is to help you effectively manage your electronic records. This goal requires the right tools, processes, technology and support. There are three main steps to get us where we need to be:



### UPDATE OUR ORCS

Making sure our Operational Records Classification System (ORCS) reflects the Commission's current business environment - the work we do now, and the records we maintain to support that work.



### IMPLEMENT THE ORCS

Run a series of Shared Drive organization projects so we are managing our records with ARCS and ORCS. This implements the ORCS, and is essentially a (really big) clean up project!



### INTRODUCE EDRMS

Once the shared drive projects are complete, and our records organized, we will be ready to onboard an Electronic Document Management System (EDRMS).

**This is where we want to be.**

Organizing our shared drives is a critical part of the IM goal. As you may have noticed, the information on our shared drives is arranged in a variety of ways right now. "Organizing," means we arrange our electronic records according to our new ORCS and to ARCS. This process allows us to:

- 1) Have our files organized in a consistent manner.
- 2) Know the requirements for managing our records, rather than just storing them forever.

Doing this will:

- increase findability of Commission information;
- support collaboration;
- assist with business continuity through staff change; and
- help us to be better stewards of the information we hold.

Applying ORCS and ARCS structure to shared drive records provides a functional logic, and consistency.

## THE 3 GOALS FOR A SHARED DRIVE PROJECT

We have three basic goals for our shared drive projects:

1. **Reduce unnecessary duplication**

Doing this helps us to focus on managing the official records, reduce storage costs, and have more efficient file searches.

2. **Reduce long file paths.**

We have a 250-character limit for file paths, which includes document names. Any file paths longer than that are at risk of not being backed up.

3. **Ensure that every folder clearly relates to an ARCS or ORCS classification.**

**And of course, create a useable environment where people can keep and find their records.**

## COMMISSION SHARED DRIVE PRINCIPLES

- Top-level folders will clearly match an ARCS or ORCS classification. All content within the folder belongs under that classification, unless otherwise indicated.
- We will use the classification title, or a close match, and follow that with the classification number. Exceptions to using the classification title will be to provide a more intuitive environment for staff.
- Folders with series of files in them will have a “Closed” folder at the top, and staff will move the closed projects, investigations, or other files into that closed folder on an ongoing basis, to assist with easy file management.
- If the retention for the folder is based on a calendar or fiscal year, folders will be established accordingly (i.e. a folder each for 2016, 2017, 2018 and so on) to make file management easier
- Staff will use naming conventions to help control versions, and identify final copies of documents.

## GETTING STARTED

### KEY ELEMENTS TO A SUCCESSFUL SHARED DRIVE PROJECT

- **Training.** Provide basic training so all affected staff understand why we are doing the project, and what we mean when we talk about retention, [transitory records](#) and ARCS/ORCS.
- **Have clear roles and processes.** Ensure everyone knows what they will be doing in the project, and what the go-forward plan is.
- **Plan it out.** Think through the details such as security permissions for the folders, what the structure needs to look like, what classifications apply, and contact your Records and Information team for advice.
- **Communicate, communicate, and communicate.** Moving people's records has to be done with care, so you don't negatively impact business or cause undue stress. Plan out the best way to communicate when files will be moved, how to help folks find the new file locations, and how to involve them in understanding the new system.

Before you get started, see the [ARCS/ORCS User Guide](#) for understanding records language, and watch our 4-minute video on [Organizing Commission Shared Drives](#)

Here is an overview of the process, and snapshots of our approach.

### HIGH LEVEL STEPS FOR ORGANIZING SHARED DRIVE FOLDERS

1. Evaluate your current structure.
2. Work with RIS to find duplicates, long file paths, and identify ARCS / ORCS classifications.
3. Plan the new structure. Set up a folder and start building the new folders within it (see the next section for how this might look).  
Considerations:
  - a. If you have existing folders that can be classified by an ARCS or ORCS category, you may just need to rename that folder with the file number on it.

- b. If you have folders with fiscal or calendar year retentions, set up a year structure inside that overall folder (example: a travel folder, with sub-folders for each fiscal year). See next section for examples, and refer to naming conventions for dated folders.
  - c. For folders that have “project” type of material, and an SO retention, put a \_Closed folder in there, so when the project is closed, it can easily be dragged and dropped into the \_Closed folder, and staff will only see active projects when they first open that space into the folder. This will keep the folder cleaner.
  - d. Create a high level folder called \_Final Disposition. When you find folders that are closed, and at the end of their lifecycle, put them in the \_Final Disposition folder, so we can process them. This is an important clean up element!  
  
**TIP:** we usually mirror your new structure in this folder, so closed files can be managed easily in the future.
  - e. Are there folders that require unique security permissions? Permissions are assigned at the root folder level, so when you are planning your structure this may affect where you put specific folders.
  - f. Often at this point the structure is in its “first phase”. Once you start going through folders you may identify new categories of records, so expect it to grow as you move through the project
- 4. Establish naming conventions. Are there specific ones for your team, beyond the standard Commission naming conventions?
  - 5. Meet with your team and go over the new structure. Have the ARCS/ORCS classifications you have used on hand, so you can speak to the retention plan if people ask.
    - a. Establish a plan to meet with team members to talk with them about “their” records, confirm classifications, and what goes where in the new structure.
    - b. Be sure to discuss the nature of the records with staff, rather than making assumptions. This is key to assigning the correct classifications, which ensures the records are findable, and will have the appropriate retention applied.
  - 6. Once everyone is comfortable with the new structure move it out to the root level. You may want to move (copy/paste) the old folder structure into a folder called something like “previous folders”, so your team sees the new structure first - and you don’t have to sort out old from new.
  - 7. When moving files, make sure you:
    - a. Find a time when staff won’t be working with the documents.

- b. Inform staff ahead of time so they know the information is moving, and tell them where the information is moving to.
  - c. Move the files at the scheduled time.
  - d. When the contents of an old folder have been moved out, assign an “x” at the front of the old folder to indicate that it’s empty. Put a shortcut in the empty folder to the new location, to help people who go to the old folders out of habit.
8. Carry on moving folders / documents into the new structure!

See the next page for examples of what this looks like.

## WHAT DOES THIS LOOK LIKE?

Here is an example of a shared drive using ARCS numbers on folders. Note that they are arranged alphabetically, by classification title, with the ARCS numbers following the title:

- 📁 Audit and review files 975-40
- 📁 Lists spreadsheets and registers 100-05
- 📁 ORCS Development 432-40
- 📁 RM projects and plans 432-60
- 📁 Travel files 1240-20

432-40 is an ARCS classification number.

**All documents within this folder fall under this number, unless otherwise indicated.**

The sub-folders within these can be free form. The expanded version looks like this:

- ▼ 📁 Audit and review files 975-40
  - 📁 Land sale audit
- ▼ 📁 Lists spreadsheets and registers 100-05
  - 📁 2010 Well files
  - 📁 Accessions
  - 📁 Industry contacts
- ▼ 📁 ORCS Development 432-40
  - 📁 Current draft
  - 📁 Planning and background
- ▼ 📁 RM projects and plans 432-60
  - 📁 \_Closed projects
  - 📁 Field and pool e-filing project
  - > 📁 LAN Organization project
  - 📁 Well file scanning project
- ▼ 📁 Travel files 1240-20
  - 📁 2017-18
  - 📁 2018-19
  - 📁 2019-20

Notice that these files are set up by fiscal year. It makes sense for finding the files by the year you travelled & claimed the expenses, and is easy to manage according to the file retention.



Here is another example:

- 📁 HR Corp Serv & HR Planning 400-20
- 📁 HR Disability Case Management 7315-25
- 📁 HR Disaster or Emergency Response Planning 275
- 📁 HR Employee Engagement Activities 7480-35
- 📁 HR Employee Work History 7385-20
- 📁 HR Employer-Employee Relations 7480

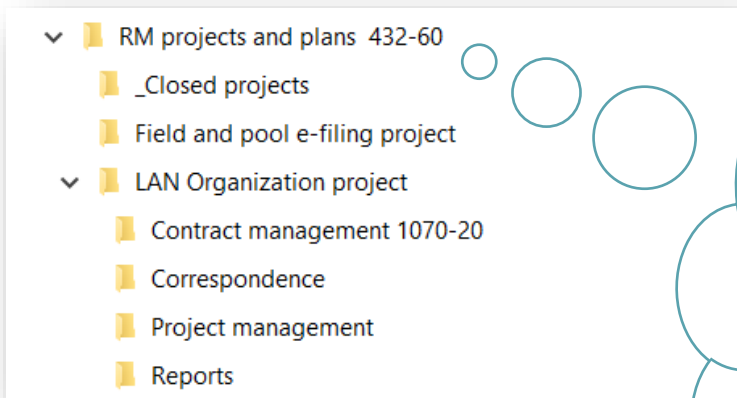
A simple primary number, not followed by a secondary number, means the folders within it have individual secondary numbers.

Per the example above, sometimes you will want to group related files together, even though they have different secondary classifications. In this case, the highest-level folder will have a primary, and inside that folder are secondary classifications:

- ▼ 📁 HR Policy & Procedure 7300
  - > 📁 Policy & procedure - development 20
  - > 📁 Policy & procedure - finals 00

NOTE: Documents are not filed in this upper level folder. **We only have documents in a folder with a secondary number on it, so we have a retention plan for it.**

Alternatively, you may nest one folder into a file which has a different classification altogether, because it makes sense operationally... this makes managing the folders a bit more complicated, but convenience and practicality may make it worthwhile. See the image on the next page:



It makes sense for the contract management material to be in the project file so the team can access it.

The LAN organization project is managed under 432-60.

The ARCS number for the contract management folder within it is in the file title to indicate there is a different retention plan than the rest of the project file.

You will see that while we are introducing structure and have some guiding principles, we are also trying to provide some flexibility so people can intuitively find their files.

---

Records and Information Services are happy to assist in the project planning process! We can help in the following ways:

- ✓ Provide de-duplication reports and long file path reports to assist in cleaning up your current drives.
- ✓ Help you find correct classifications for your information, which will form the basis of your new structure.
- ✓ Advise on best practices for naming conventions, if you think those would help your team.
- ✓ Provide templates for folder management tips, or cheat sheets, and
- ✓ Cheer with you for your progress!

*Please contact Records and Information Services if you are ready to start a shared drive project, or if you have questions about our records program initiatives.*

*And check out our resources on our [MyOGC Information Management](#) page.*

## Shared Drive Organization Projects Selection criteria

We weight the selection for shared drive organization projects accordingly:

Criteria	Description
<b>Branch Readiness</b>	Branch Readiness looks like this: <ul style="list-style-type: none"> <li>• Branch can provide a primary contact for the project</li> <li>• Staff have time to attend training and planning sessions, and</li> <li>• Staff can meet with RIS on an as-needed basis.</li> </ul>
<b>ORCS Implementation</b>	A priority for RIS is to implement the ORCS. This supports: <ul style="list-style-type: none"> <li>• momentum from the ORCS modernization project,</li> <li>• continuity for staff who have already been thinking about records, and</li> <li>• provides value for time spent on ORCS development.</li> </ul>
<b>Location</b>	We want to share our work to all corners of the Commission, and may prioritize a project if it is in a location that we have not directly supported recently.
<b>Business Cycle</b>	It is critical to project success to align with natural ebbs in business cycles; we want to be careful not to start a project during “crunch times”.
<b>Complexity of project</b>	If we have a small gap of time, we may prioritize smaller projects that we know we can complete in the time available.



# Shared Drive Organization Engineering project

Presenter:

Mahia Frost, OGC Information Management Specialist

Special Guest:

Marion Villines, Shared Drive Organizer Extraordinaire

## Shared Drive Organization

Project drivers – PGA and IMA requirements

Overview of your shared drive

Going forward

- (a) correspondence,
- (b) investigations,
- (c) surveys,
- (d) reports,
- (e) data,
- (f) background information,
- (g) assessments,
- (h) designs,
- (i) specifications,
- (j) field reviews,
- (k) testing information,
- (l) models,
- (m) simulations,

Bylaws of Engineers and Geoscientists BC





## Shared Drive Overview

### Project goals:










- All folders have an ARCS/ORCS classification at the top
- All documents within a folders belong to that classification/topic

- 📁 \_FINAL DISPOSITION
- 📁 \_PREV FOLDERS
- 📁 \_SHARED DRIVE TOOLS
- 📁 200-20 Committees
- 📁 20000-02 Analysis Projects
- 📁 20000-40 Compliance Monitoring
- 📁 20550-10 Audits - Final Reports
- 📁 20550-20 Audits - Working
- 📁 20550-20 CAP
- 📁 21000-35 NOI Repair in Kind
- 📁 21000-35 Pipeline Pressure Tests
- 📁 21100-00 Policy & Procedure - Finals
- 📁 21100-20 Policy & Procedure - Dev
- 📁 21250-10 Initiatives
- 📁 21600-20 Annual Activity Reports - Finals
- 📁 21600-30 Annual Activity Reports - Dev

## Standard Folders

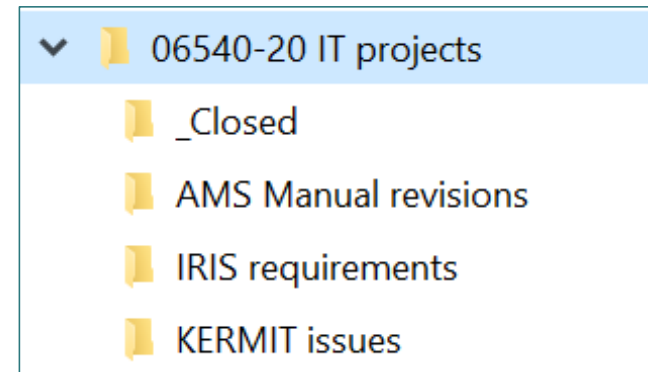
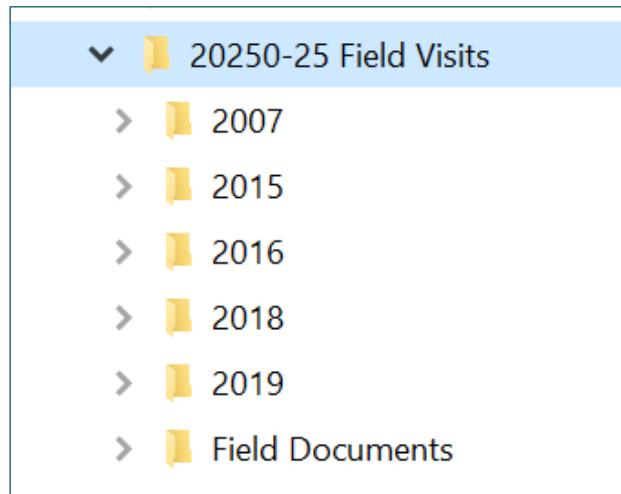
\_FINAL DISPOSITION

\_PREV FOLDERS

- ▼  \_PREV FOLDERS
-  x Aged assets IMP project 2018-19
- >  x Commission Shared
- ▼  x Engineering & Geology
  -  x Files - Ivy Chan
  -  x Incidents Spreadsheet
  - >  x Integrity Management
  - >  x Engineering Kelowna
  - >  x NASH



**Some of the ways we organize documents in the folders.**



## Using the system

Focus on what you are doing to find the right home for your information.

- 📁 \_FINAL DISPOSITION
- 📁 \_PREV FOLDERS
- 📁 \_SHARED DRIVE TOOLS
- 📁 200-20 Committees
- 📁 20000-02 Analysis Projects
- 📁 20000-40 Compliance Monitoring
- 📁 20550-10 Audits - Final Reports
- 📁 20550-20 Audits - Working
- 📁 20550-20 CAP
- 📁 21000-35 NOI Repair in Kind
- 📁 21000-35 Pipeline Pressure Tests
- 📁 21100-00 Policy & Procedure - Finals
- 📁 21100-20 Policy & Procedure - Dev
- 📁 21250-10 Initiatives
- 📁 21600-20 Annual Activity Reports - Finals
- 📁 21600-30 Annual Activity Reports - Dev

## Best Practices



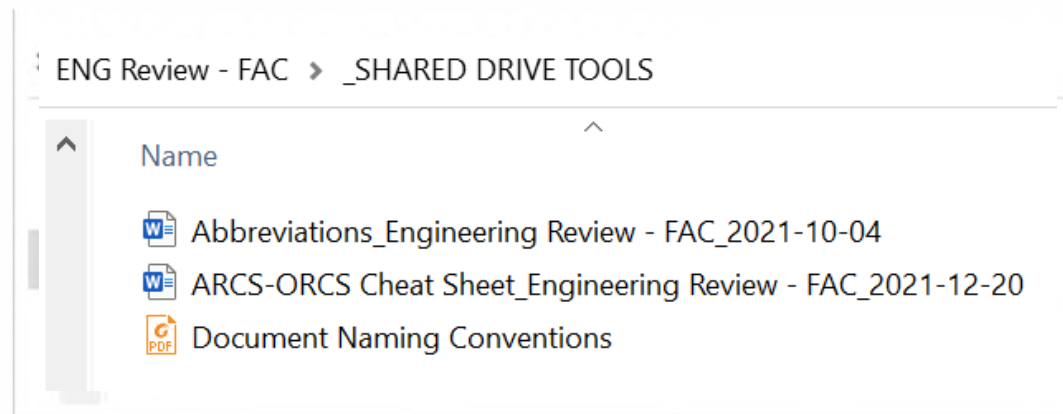
Keep contents clean  
– delete transitory  
material.



File relevant emails  
into folders so you  
have a whole record.

## Standard Folders – Shared Drive Tools

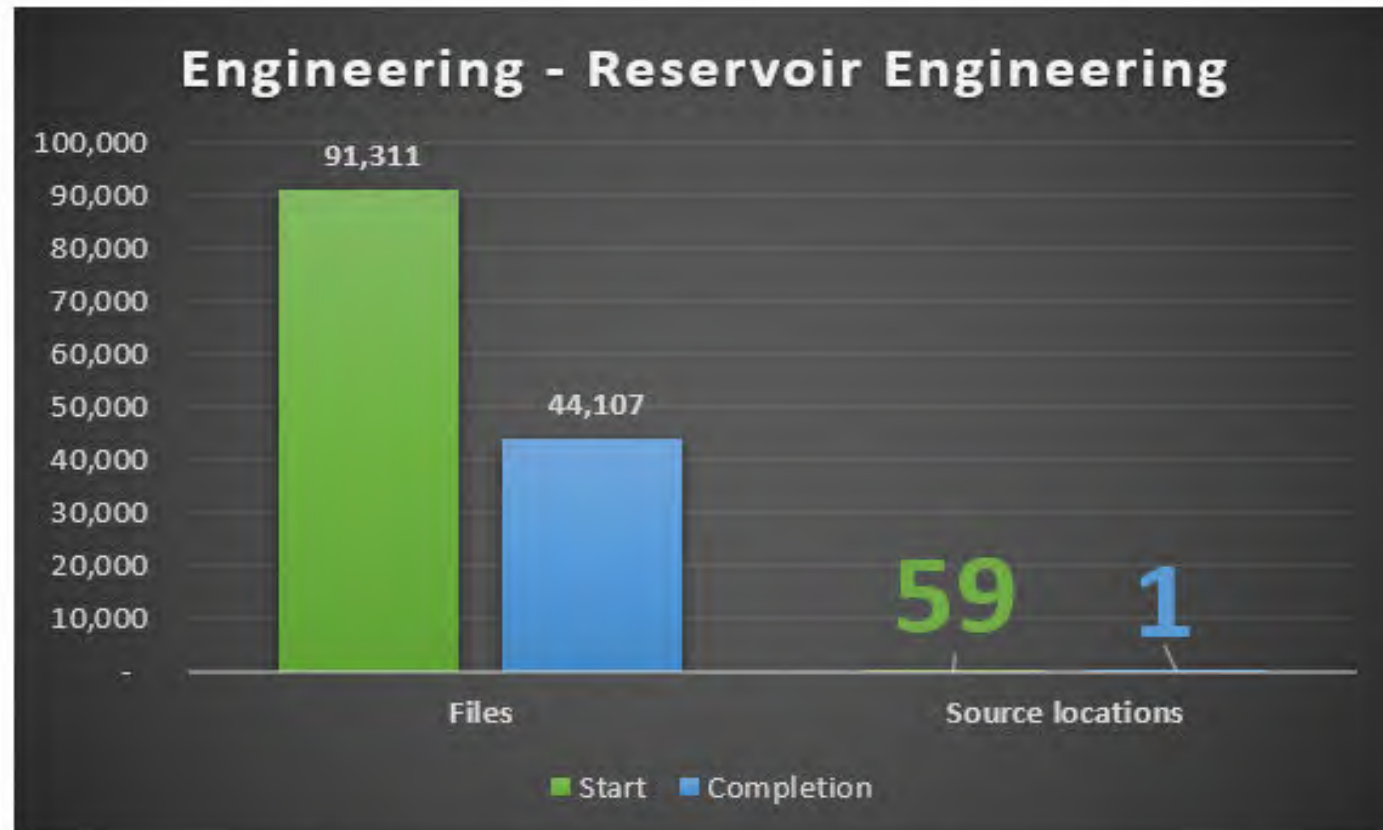
### \_SHARED DRIVE TOOLS



**What to do next.**



YOU JUST HAD A BIG  
"HOUSECLEANING"!



Review of records dating back to 1996 - 26 years of electronic information!  
Eliminated duplicate and obsolete records: **52% reduction** in files/documents.  
Harmonized records from 59 sources to (basically) one place.  
Project duration: 5 months, including pre-project analysis time.  
**Fantastic involvement and support from the Reservoir Engineering team!**

## Engineering - Reservoir Engineering

YOU JUST HAD  
"HOUSECLEANING"



1  
source locations  
electronic information!  
in files/documents.

Harmonized records from 59 sources to (basically) one place.

Project duration: 5 months, including pre-project analysis time.

**Fantastic involvement and support from the Reservoir Engineering team!**



# RM Resources

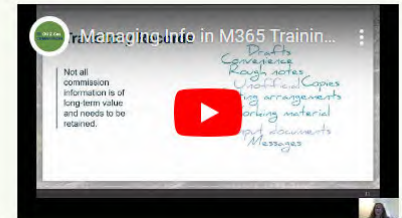


## Information Management in M365

Microsoft 365 offers new tools for creating and using our information, but the Information Management rules haven't changed. Here is some guidance on how we manage our information in the M365 environment.

- [Managing Information in Teams](#)
- [Managing Information in OneDrive](#)
- [Managing Information in SharePoint](#)
- [Teams - Sharing Documents in Teams](#)
- [Teams - Saving Documents from Teams to Shared Drives](#)
- [Teams - Saving Meeting Recording to Shared Drives](#)
- [Teams - Documenting Chats](#)

Our Interim Policy for [M365 Information Governance](#) outlines the Commission's approach to managing information in these tools as we adopt and adapt to this platform.



Managing Information in M365

### Workplace Essentials

+ New Send to Promote Page details Immersive Reader Analytics

## Information Management

### All things related to managing information in the Commission

There are many considerations when managing our business information. We have provided resources to help you understand your responsibilities, and the Information Management tools to help you.

#### On This Page

<a href="#">Transitory Records</a>	<a href="#">Email Management</a>	<a href="#">Top 5 "Basics" for Managing Information</a>
<a href="#">Documenting Commission Decisions</a>	<a href="#">IM in M365</a>	<a href="#">Shared Drive Organization Project</a>
<a href="#">IM Resources</a>		

#### Links

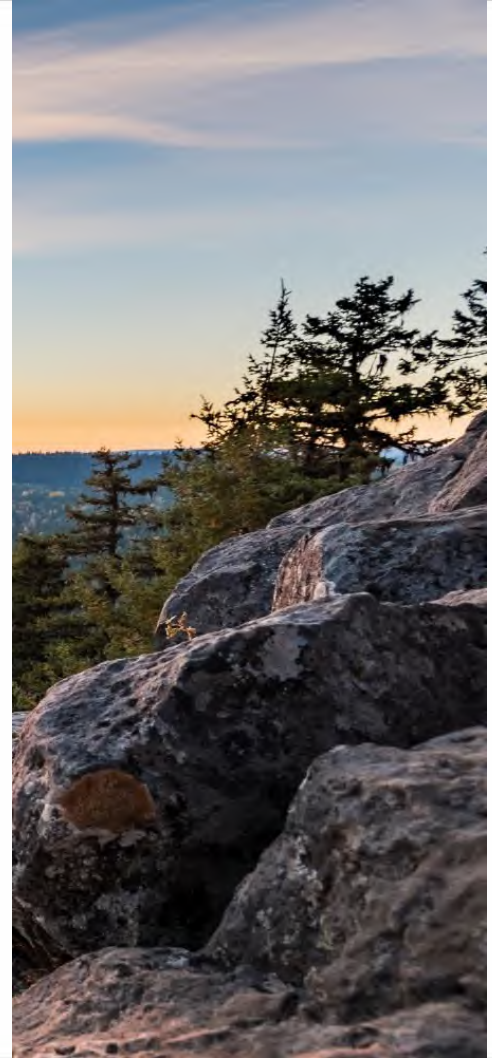
- [ARCS Online](#)
- [Oil and Gas Regulation ORCS](#)
- [Human Resources ARCS](#)
- [Information Management Act](#)
- [Documenting Decisions Directive](#)
- [OGC FOI and Protection of Privacy page](#)



Please reach out with any questions



*Thanks for working with us!*





Copy and paste this '3' onto any slide you wish. It will automatically populate to the correct slide number. 



# Managing Email Guide

June 2021

# Table of Contents

Overview	3
Using your Commission email	4
Using personal email accounts	4
Tips for sending email	6
Tips for managing email discussion threads	7
<b>Managing your email</b>	
Commission emails are Commission records	8
Deciding what to keep or delete	8
Organizing email in Outlook	10
Working with Folders	10
Working with Categories	11
Working with Rules	12
Saving email records outside of Outlook	12
Saving email – Responsibilities	13
Tips for saving email records	13
Preferred email preservation formats	14
Saving email records on your Shared Drives	15
Deleting email appropriately	15
Working with the Clean-up tool	16
Working with Auto-Delete folders	17
Working with Assign Policy tool	17
Emptying Deleted items on exit	18
Exercise: Find and delete emails from distribution lists	18
Contacts	20
Appendix A: Managing Phishing and Spam Quarantine	21

# Overview

Email is a fundamental communication tool for Commission employees. The volume and diversity of the emails we create and receive on a daily basis can make managing them seem like an impossible task. This guide will help you navigate the world of email so it can be as effective a tool as possible.

Good information management practices can help you manage your emails. Implementing simple routines will help you to wade through your emails and separate the valuable messages from the rest. Proper email management will not only make your life easier, it will ensure that important commission information is available to meet business and legislative requirements.

This guide will help you to comply with the [Freedom of Information and Protection of Privacy Act \(FOIPPA\)](#), the [Information Management Act \(IMA\)](#), our [Information Management Policy](#), and [Use of IT Resources Policy](#), including how to:

- understand security responsibilities surrounding email
- understand your responsibilities when using your email account
- determine what emails need to be kept and keep those emails in ways that protect their authenticity and integrity
- determine what emails you can delete
- delete those emails appropriately using simple tools available in MS Office 2016 for Windows

*Much of the material in this guide originates from the BC Government Records Service. The Commission version is a collaboration between Information Systems & Technology, and Records & Information Services.*

# Using your commission email

## ***When do I have to use my commission-issued email account?***

As an employee, you are required to use your commission email when conducting commission business (except in extenuating circumstances).

Not all of our business requires the use of email — but when it does, you are required to use a commission account. This includes when you are working outside the office.

## ***Can I use my personal email account or an email account related to another organization for personal use while at work?***

Per the [Use of IT Resources Policy](#), reasonable personal use of commission-issued IT device by employees is permitted as long as you follow these rules:

- Your use of non-commission email account on a commission- issued device should be limited during work hours and must not interfere with your duties and responsibilities.
- Any use of personal email for personal use while at work must be lawful, must not compromise the security of commission IT resources or commission information, and must not be used for personal financial gain.
- The use of a commission-issued computer, laptop, smartphone or other device must be consistent with the [Employee Oath of Conduct and Ethics](#), whether that use is directly related to your employment duties or not.

# Using personal email accounts

## ***Can I ever use my personal email account for work purposes?***

Only in rare, extenuating circumstances are you permitted to use a non-commission email account for commission business. It must be absolutely necessary to do so.

For example, you may not forward work emails or documents to your non-commission email account simply to work on them at home or to create a convenience copy.

In the rare circumstances where you are unable to securely access your commission email account, you must always follow these steps:

- Send or receive the least amount of confidential information necessary to deal with the extenuating circumstance until you are able to use commission email again.



- Send a copy of the email to your commission email account. A good practice at this step is to note the circumstances that prevented you from accessing your commission email account.
- Delete the email from the inbox, sent items and trash of your non-commission email account as soon as possible. You should also send an email note to your commission email account noting that you have deleted the commission record(s) from your personal email account and have not made any copies of the information.
- Resume use of commission email as soon as possible, including using commission email for the remainder of an interaction that began via personal email.

You must exercise additional caution if the email contains personal information. Most email account providers – such as Gmail or Hotmail – store your emails outside of Canada and the *Freedom of Information and Protection of Privacy Act* prohibits personal information held by the government from being accessed or stored outside of Canada, except in limited circumstances.

## A word on protecting sensitive information...

You are responsible for ensuring that any confidential information you are working with is protected. Email is not a secure communication channel. Given the ease with which email messages can be distributed and accessed by others, you need to take extra precautions when working with confidential information.

Limit the amount of confidential information transmitted over email. Use your best judgment or, if you are uncertain, check with your supervisor. Avoid using email to send confidential, sensitive, protected or secret information, except where there is a specific business requirement to do so.

See our [Managing Confidential Information Guide](#) for more information, or call Records and Information Services if you have a question.



### Why this is Important

Protects confidential or sensitive information that is often accessible to us as part of our work, and for which we are the trusted stewards.

# Tips for Sending Email

- ✓ Keep email to a single topic. If the topic changes, create a new email thread. If the email covers two or more topics, consider filing it in two places.
- ✓ Be specific in the subject line. Create a clear, concise, and descriptive title. Use the subject line to indicate actions, purpose and due dates.
- ✓ Use your signature block for all outgoing email messages going to recipients outside your working group. If your email contains important decisions or actions, always include your signature block.
- ✓ Limit the number of recipients. Only include recipients who are expected to take action or make a decision on a topic. Use the 'cc' option when sending messages to recipients for informational purposes.
- ✓ Limit the use of attachments. Whenever possible, post your document to a shared location (e.g. on shared drives) and send a link in the email (see [Appendix A](#) at the end of this guide for how to insert a hyperlink into an email)

Descriptive subject lines are important for managing email and are helpful aids for determining whether you need to save an email or if you can delete it. Some recommended subject lines are:

**Action by <date>**

**Follow up:**

**Question:**

**Answer:**

**Request:**

**As requested:**

**As promised:**

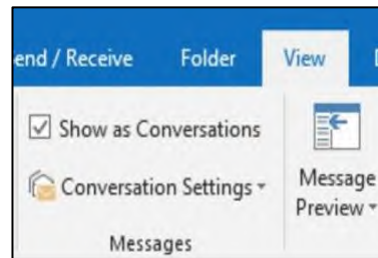
**FYI**

**Thank you!**



# Tips for Managing Email Discussion Threads

- ✓ Do not forward unnecessary information from previous emails to new recipients. Before you include another person on the thread, delete any information that is not needed for completing the task at hand. Avoid unnecessary duplication.
- ✓ Recommended practice: the person who initiates the email thread be responsible for ensuring the thread gets filed. Recipients may also save emails, depending on the content and context of the message.
- ✓ Use the conversation clean-up tool with caution. When a conversation has split into separate conversations, the system may delete intermediary emails that are older than the final email in the collection. Be sure to assess and mark important decision emails prior to running the tool.
- ✓ Don't share personal information unless it is necessary for completing the job at hand. Keep personal information on a need-to-know basis. Share only the right information with the right person for the right purpose
- ✓ Set your Outlook to 'Show as Conversations'.



# Managing your email

## Commission Emails are Commission Records

Emails pertaining to the business of the commission are considered commission information, and as such, must be managed for set time periods, and possibly kept permanently.

Information schedules approved under the *Information Management Act (IMA)* provide classifications and timelines for managing all government information. Emails should only be deleted or disposed of in accordance with approved information schedules (i.e. ARCS and ORCS) and should not be subject to periodic and indiscriminate deletions.

As an employee, you are responsible for filing emails that document commission activities and decisions in the appropriate recordkeeping system (e.g. a shared drive, organized according to ARCS and ORCS).

Remember that your email account is a communications tool, not a place to manage records.

For more information on filing emails see the section on [Saving Emails Outside of Outlook](#).

## Deciding What to Keep or Delete

*Do I need to keep every email? When can I delete an email?*

You need to save all emails that pertain to the business of the commission, except for transitory emails. Transitory emails contain information of temporary usefulness that is needed only for a limited time, to complete a routine action or prepare a subsequent record. You may delete transitory emails when they are no longer needed.

You must not delete any emails that may be responsive to an active FOI request or request for legal discovery.

You should save emails that document an important government decision. For more information on the duty to document decisions, see the [Guidelines on Documenting Commission Decisions](#).



Save Official Email Records



Delete Transitory Emails

## Keep or Delete

### Examples of official emails (that must be saved and managed):

- emails that document business transactions (initiation, authorization, or completion)
- emails that document decisions, including instructions, approvals, advice, and signed briefing notes
- emails that document a policy decision, significant action, or how a case was managed
- formal communication about commission business
- emails that contain information that is integral to a file about one event, client, or issue (e.g. a case file)
- legal advice and agreements
- unread email that is evidence of attempted consultation
- emails that contain other information that helps explain the history of a relationship, decision or project

### Examples of transitory emails (which can be deleted):

- announcements of social events
- cc copies (unless you are the main staff member responsible for the matter)
- emails conveying an attachment (if it doesn't add value to the attachment)
- meeting arrangements
- routine correspondence about drafts and revisions
- a request to call someone
- personal emails such as lunch/coffee arrangements and birthday wishes

## Decision guidance

1. Is this email needed for your work?  
(Does it provide evidence of official business, policies, actions, transaction, or decisions?)
2. Does it hold a final document not kept elsewhere in the recordkeeping system?
3. Is it a draft/revision with information on decisions/approvals not found elsewhere?
4. Is it working material essential to understanding final documents?
5. Are you the main, or only, recipient for the commission?

If the answer is **yes** to any of these questions, then the email should be **saved**.

If the answer is **no** to all of these questions, then you can **delete the email** as a transitory record.

For more information on determining if you should keep or delete an email, see our [Email Decision Diagram](#) and our [Official vs Transitory Records](#) guides.

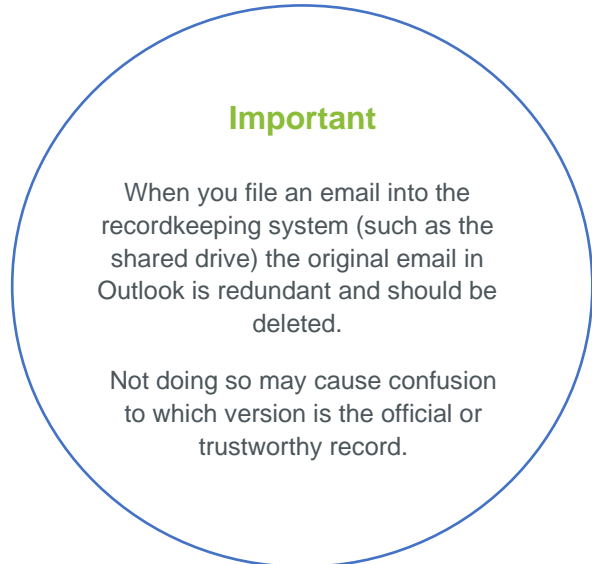
# Organizing Email in Outlook

*My inbox is a mess! How can I manage all my emails?*

An unruly inbox will seem daunting to many. Organizing your email inbox is fundamental for proper email management. Aim to identify and act on emails as soon as they arrive in your inbox.

This section will guide you through a number of useful tools you can use to organize and classify your emails in Outlook 2016 for Windows (some of these features may not be available for other versions of Outlook). The tools include:

- **Folders**
- **Categories**
- **Rules**



## Working with Folders

It may be useful to think about email management in the context of paper practices. In the pre-internet era, messages would arrive to your office inbox in paper form. They wouldn't just stay in that inbox; you would read the messages then either file them away or dispose of them. The inbox was a temporary storage location, not a final destination. The same is true of your Outlook inbox today.

As a rule, employees should file or delete their email as soon as possible after sending or receiving them. However, this isn't always possible or desirable. Creating custom folders in Outlook to organize your inbox will help you file and delete emails in a timely manner.

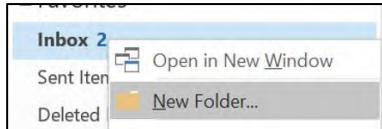
**Best Practice:** It is recommended that you create Outlook folders according to classifications in information schedules (i.e., ARCS and ORCS). Use the file code (ARCS and ORCS primary and secondary numbers) in the folder name. Create a folder for each project you are working on or create a subject-based folder. Create as many sub-folders as you need. If you decide this, contact Records and Information Services for assistance with ARCS and ORCS.

If that seems like too much right now you can get halfway there and set up folders for specific topics or parts of your job, and that will still put better order in your Outlook.

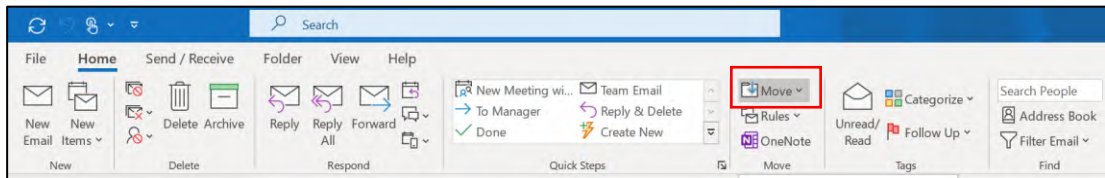
It is also good practice to create a transitory email folder for items that are of temporary usefulness. You can apply rules to the transitory folder to delete transitory emails after a specified period has elapsed. See the section on [Deleting Emails Appropriately](#).

**To create a new folder:**

1. Right-click the **Inbox** folder in the navigation pane and choose **New Folder**. Type the new folder name and press **Enter**.



2. Drag and drop messages from your Inbox into the new folder, or, use the **Move** button to move the email into a folder (you can pick from a drop-down list of recently used folders)

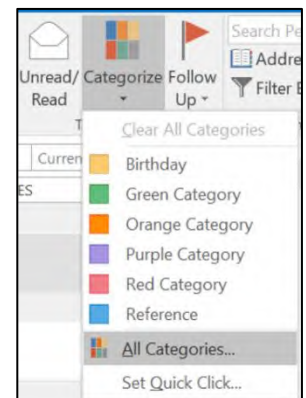


## Working with Categories

Colour Categories in Outlook are another useful way of organizing your inbox. Not only do colour categories allow you to visually identify your emails at a glance, but you can use them to perform quick sorts, populate search folders and much more.

Outlook has a number of default categories which have been named according to their colour. You can customize them to categories that make sense to you.

1. Click the **Categorize** button in the upper ribbon to open the list of categories.
2. At the bottom of the drop-down list, choose the option to view all categories. In this pane you can add or delete categories, or rename them according to your preference. Choose categories that work for you, such as Action, To Read, etc..
3. Go back to your Inbox, click on the email to highlight it, then click on the **Categorize** button again, to select the category from your list (right clicking on the email also brings up the **Categorize** option).

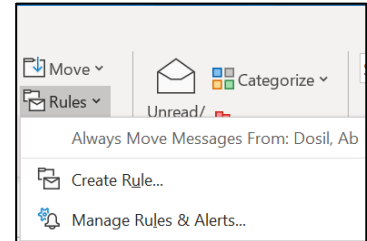


## Working with Rules

Rules can be useful for automatically moving email to a specified folder. If there are specific people, subjects, categories, or topics that will always go in the same folder, you should set up a rule that automatically routes those emails to that folder.

### To set rules:

1. Click on the **Rules** button in the upper panel to open the drop-down menu.
2. Select **Manage Rules and Alerts**.
3. In the **Email Rules** tab, select **New Rule**. This will allow you to choose from a number of rule templates that you can customize, or you can create your own rules from scratch using the **Create Rule**.



## Saving Email Records Outside of Outlook

A recordkeeping system is a shared filing system in which records, including government emails, are managed in accordance with approved information schedules. A recordkeeping system, when used in conjunction with recorded policies and procedures, defined roles and responsibilities, and on-going training, constitutes an appropriate system for managing government information.

An appropriate recordkeeping system should:

- contain logical, organized naming conventions that can be followed by all staff;
- ensure the preservation and accessibility of records over time;
- protect against accidental or unauthorized access, alteration, copying, movement or deletion;
- minimize duplicate storage of records; and
- permit the retention requirements of information schedules to be applied accurately and efficiently.

This section will provide guidance on how to save emails to your office's recordkeeping system. It will walk you through:

- **Saving email – responsibilities**
- **Tips for saving email records**
- **Preferred email preservation formats**
- **Locations for saving emails**

## Saving Email – Responsibilities

### **Managing email is the responsibility of every employee**

It is the responsibility of all staff to manage their emails appropriately. You should identify emails that are records of your business activity, move them out of your Outlook mailbox, and manage them alongside related records in your office's recordkeeping system.

### **The email sender is responsible for saving internal email**

It is the responsibility of the sender of an email or the initiator of a dialogue to decide if the email and/or attachment(s) constitute an official record. If the email or its attachment(s) contain key decisions and/or actions taken, it should be considered a record, renamed (if appropriate), and saved in the most appropriate place.

### **The principal receiver is responsible for saving external email**

If you are the sole recipient of an external email or, if there are several recipients, and you are responsible for the most relevant work area, you are responsible for deciding if the message forms part of an official record or not and taking responsibility for its management.

### **Working groups should assign responsibility for shared mailboxes**

When managing emails in a shared mailbox, working groups should be clear as to who is responsible for the retention, naming, capture and disposal of emails within the mailbox. Without the identification of clear responsibilities, emails may be lost or duplicated. It is recommended that the folder owner take responsibility for a shared mailbox.

## Tips for Saving Email Records

A complete record includes sufficient content, context, and structure to ensure that the information can be accessed, understood, and preserved for as long as necessary, and that its value as evidence will be maintained. To do this, you need to preserve all elements of the email, including the email header, the message body, and any attachments.

- To prevent a loss of information, move emails to an appropriate location as soon as possible.
- It is not necessary to capture every email in an email conversation thread separately. Instead emails should be captured at key points during the conversation, when key decisions are made and transactions processed.
- Email attachments should be saved as part of the record to provide context to an email. However, there will be occasions when it won't be necessary to capture both the email

and its attachment. For example, if an attachment has been sent for reference purposes and you know it has been captured elsewhere.

- If the title of the email does not accurately reflect the content of the message then it should be re-titled at the point at which it is saved. Renaming email records is particularly important when they represent different points in an email string as it will identify the relevant aspects of the conversation.
- Consider dating the email in the title before saving it. For government bodies who receive a high volume of requests under FOIPPA, the ability to sort by date is particularly important. Use the format YYYY-MM-DD to date your emails in the title.

## Preferred Email Preservation Formats

**For filing on the Shared Drive: .MSG**



MSG files are the native Outlook format. When you drag and drop an email to your desktop or to a LAN folder, this is the file format that is exported. Outlook can export calendar items, emails, contacts, and other Outlook content via MSG. This format is preferred because all header information, message content and attachments are preserved with the file. The file will retain a lot of its original functionality when reopened.

**For filing anywhere (ideal for long-term storage): .PDF**



Emails can be exported from Outlook by printing them to a standard PDF file or a PDF portfolio. PDF files are stable and generally well supported, making them the de facto preservation standard for documents. The Adobe PDF conversion plug-in is available when you download Adobe Acrobat. This allows for one-click conversion of Outlook content to PDF.

You can also save attachments embedded in a PDF, just like an email; however, this method can cause compatibility issues. Best practice is to download the attachment and save it with the email content to ensure it can be opened in the future.



## Saving Email Records on Your Shared Drives

Saving email to a shared folder on your office Shared Drive network is our best option until we have an EDRMS. To do this, simply:

- Copy and paste the email from your Outlook to the shared folder. This will save it as an MSG file.
- Right click on the message and click **Properties**.
- Check the **Read-Only** box, click **Apply** and **OK**. This will ensure that the message cannot be edited by others.
- You can also save your emails as PDFs on a shared drive folder. Saving email PDFs and their attachments separately is recommended. While it is possible to embed the attachment within the PDF, this method is not stable and attachments can be difficult to open later. The ability to open and inspect attachments is critical for proper email preservation.

## Deleting Email Appropriately

Now that you know what constitutes an official email record and how to save them properly, you should delete the redundant (duplicate) emails from your Outlook. You are also encouraged to delete transitory emails, personal emails and other non-record reference material that is taking up valuable space.

Deleting emails quickly and appropriately ensures that your inbox will remain clean and clutter-free.

This section will provide guidance on simple Outlook tools that will help you to delete your emails appropriately. It will also include simple exercises you can perform to find and delete common categories of transitory email.

Tools include:

- **Clean-up Tool**
- **Auto-delete Folders**
- **Assign Policy for transitory emails**
- **Empty Deleted Items on Exit**
- **Exercise: Find and Delete Emails to Distribution Lists**
- **Exercise: Find and Delete Meeting Requests**

**NOTE: You are prohibited at all times from 'triple-deleting' emails (i.e. attempting to purge an email from your 'Recover Deleted Items' folder).**

This should not be confused with double deletion, which happens when deleted emails are cleared from the 'Deleted Items' folder. The double deletion process is important for clearing

space in your Outlook account, but must only be done if the items in question are permitted to be disposed of.

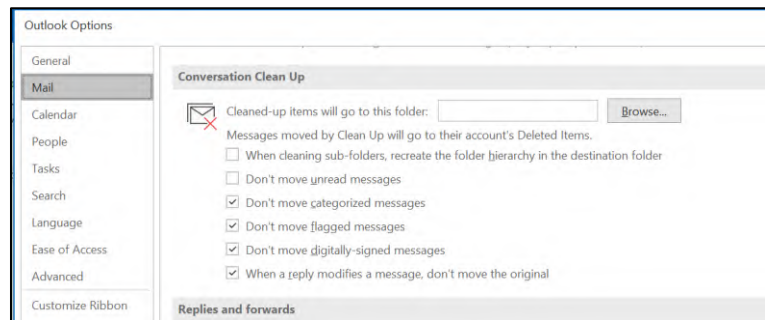
## Working with the Clean-up Tool

Email threads (termed “conversations” in Outlook) can be long and cumbersome. As people reply to the email thread, the existing content is automatically included in each response, resulting in a lot of redundant information. The Clean Up tool scans conversations and removes any redundant emails from the thread.

Before cleaning up a conversation, ensure that important emails are flagged or categorized.

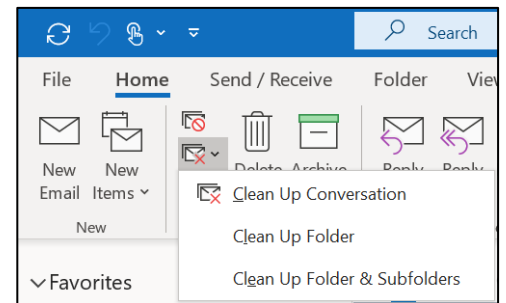
### To set the parameters of the Clean Up tool:

1. Click **File**, then **Options**.
2. In the Outlook Options pop-out window, select the **Mail** tab on the left and scroll down to **Conversation Clean Up**. By default, all cleaned up items will go to the **Deleted Items** folder. You can change this destination folder if you would like them to be routed elsewhere. There are options that allow you to prevent certain classes of email from being cleaned. Ensure that flagged emails and categorized emails are not cleaned.



### To run the Clean Up tool:

1. Highlight the folder you would like to clean. Click **Clean Up**.
2. From the dropdown menu, there are 3 options: run the clean up tool on a single folder; on a folder and its subfolders; or on specific conversations.
3. It is recommended that you run the conversation cleanup tool regularly as part of your work routine.



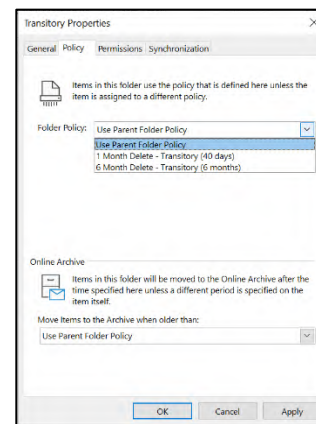
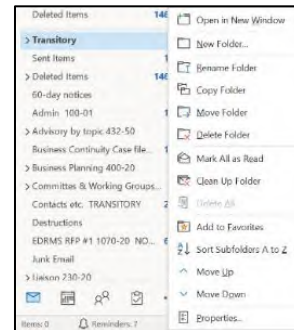
**Use caution with this tool, and refrain from cleaning email threads that may contain important information.**

## Working with Auto-delete Folders

As mentioned in the section on Folders, setting up a Transitory Folder is recommended to keep your inbox clear. You can set Outlook Rules to auto-route certain classes of transitory emails directly to this folder. There is also the option of configuring this folder to permanently delete transitory emails after a specified period. Automating this process encourages you to think critically about what is transitory and what is an official record.

To configure this setting:

1. Highlight your **Transitory Emails** folder in the left navigation pane, and right click on the folder to open the drop down menu.
2. Select **Properties**.
3. In the pop-out window, select the **Policy** tab.
4. In the drop down menu beside **Folder Policy**, select the term for how long you want your transitory emails to remain in the folder. One month is recommended. Click **OK**. Your transitory email folder will now auto-delete items that are older than one month.

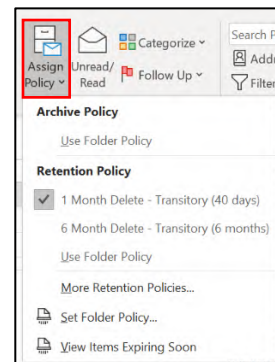


## Working with Assign Policy tool

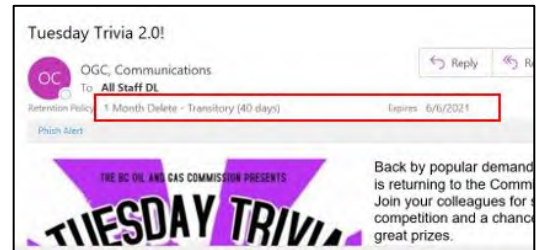
You can also assign an auto-delete policy to individual transitory emails right in your inbox or other folders. This will permanently delete the selected emails after a specified period. When you do this, think about the value of the record - whether it is transitory or an official record - and once you assign the policy, you don't have to think about it again.

To apply the policy directly to an email:

1. Select the transitory email and click on the **Assign Policy** button.
2. Choose the retention you prefer for the email from the picklist.



3. Notice the email now states your chosen retention period, with the “expires” (deletion) date. When the email reaches the expiry date it will be automatically deleted, and moved to your Deleted Items folder.



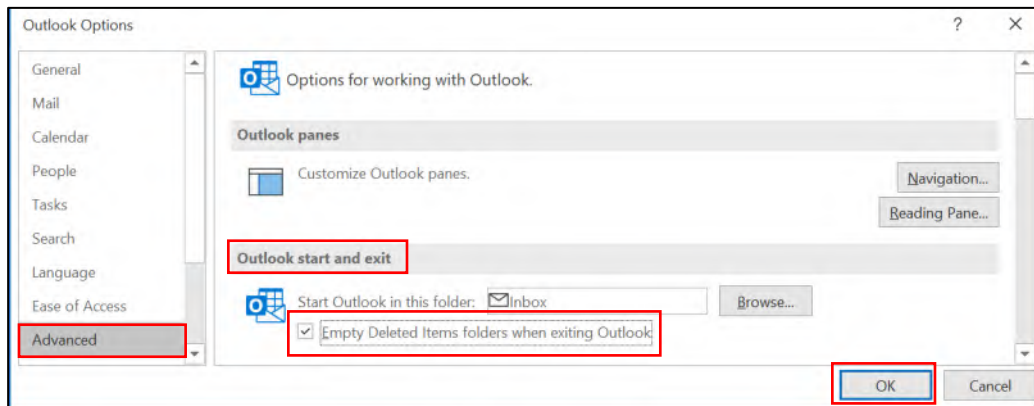
**NOTE:** Once a retention policy is applied, you cannot remove it. If you change your mind and need to retain the email for longer you can click on **Assign Policy** and extend the retention to the 6 month option. Also, if you save the email to a folder on the shared drive, the transitory retention will be removed.

If an FOI or legal matter arises your transitory records are within search parameters, and your auto-deletion will be suspended until the matter is closed.

## Emptying Deleted Items on Exit

Clicking Delete in Outlook does not permanently delete the email; it sends it to the Deleted Items folder. In the default settings, this folder will not be emptied unless you do so manually. However, you can configure Outlook to empty your Deleted Items automatically when you exit the application. This is the recommended option.

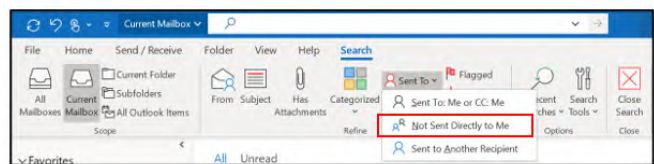
1. Click **File**, then **Options**.
2. Choose the **Advanced** tab on the left side. Under the “**Outlook start and exit**” heading, check the box that says **Empty Deleted Items folder when exiting Outlook** and press **OK**.



## Exercise: Find and Delete Emails from Distribution Lists

Emails received through internal distribution lists are another type of transitory email. As the receiver, you are generally not responsible for filing emails received through a distribution list (although you may want to keep a copy for reference purposes). To find and delete all emails that are not sent directly to you:

1. Click the **search bar** to open the **Search** tab and menu.
2. Select **Sent To**, to open a dropdown list. Click on **Not Sent Directly to Me**. This should return all emails sent through distribution lists.



**Always exercise caution before deleting large quantities of email.**

## Related Policies

- ✓ [Employee Code of Conduct and Ethics](#)
- ✓ [Information Management Policy](#)
- ✓ [Information Security Policy](#)
- ✓ [Mobile Device Policy](#)
- ✓ [Use of IT Resources Policy](#)
- ✓ [Workplace Appropriate Use Policy](#)

## Contacts

If you would like more information regarding this guide please refer to the table below.

Commission Contact	When to Contact	Email
Records and Information Services (Records Management) <a href="#">MyOGC Information Management Page</a>	For inquiries on how to manage government information.	<a href="mailto:servicedesk@bcogc.ca">servicedesk@bcogc.ca</a>
Records and Information Services (FOIPPA and Privacy) <a href="#">MyOGC FOI Page</a>	For general inquiries, or to report a privacy breach.	<a href="mailto:FOIintake@bcogc.ca">FOIintake@bcogc.ca</a>
IT Service Desk <a href="#">Service Desk</a>	For technical support or ensuring your mobile device is encrypted.	<a href="mailto:servicedesk@bcogc.ca">servicedesk@bcogc.ca</a>
Cybersecurity <a href="#">MyOGC Cybersecurity Page</a>	For general inquiries, or to report an incident of phishing, cybersecurity attacks, or a data breach.	<a href="mailto:servicedesk@bcogc.ca">servicedesk@bcogc.ca</a>
Human Resources <a href="#">MyOGC Human Resources (HR) Page</a>	For general inquiries about the Code of Conduct and Ethics.	<a href="mailto:servicedesk@bcogc.ca">servicedesk@bcogc.ca</a>

# Appendix A: Managing Phishing and Spam Quarantine

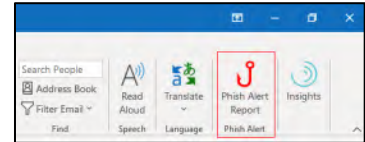
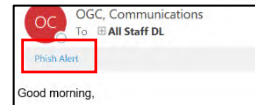
We all have a role to play in protecting the Commission and our information assets. Here are some tools our cybersecurity team has implemented to help protect us from malicious email activities.

## Managing Phishing Emails

If you receive an email that that you consider to be a phishing or other cybersecurity threat, you need to report it by using Phish Alert in Outlook. Reporting an email using the Phish Alert tool will delete the email and send a copy to Cybersecurity for analysis.

While we are transitioning to M365 you will see either of these two actions for reporting a suspicious email:

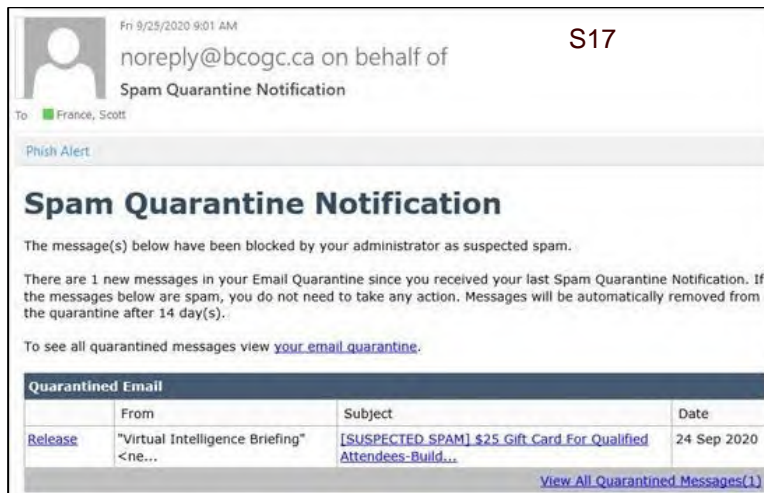
1. Click on the Phish Alert banner at the top of your email, or
2. Click the **Phish Alert Report** button located on the **Home** toolbar.



Both actions will report the email as a potential malicious email, and quarantine it by removing it from your Inbox.

## Managing Spam Quarantine Notifications

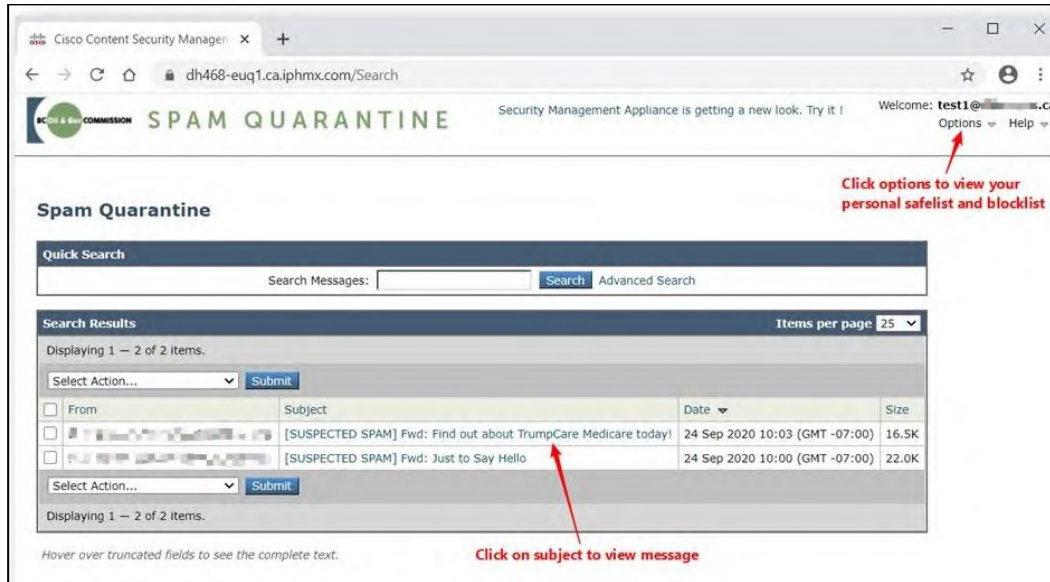
On occasion you may receive email notification of an email that has been moved into your spam quarantine. If an inbound email is suspected of being spam, our spam filter will move it to quarantine, rather than deleting it, and you will receive this notification email in the next business hour.



Hover your mouse over the links, and note the not so user-friendly domain name **dh468-euq1.ca.iphmx.com** the links point to. This is safe and will bypass the Second Chance confirmation popup when you click links in Spam Quarantine Notification emails.



To get more information about the quarantined message, click on the [View All Quarantined Messages](#). There is no need to sign in as authentication is done using a custom URL. This also means that staff working with shared mailboxes can manage the spam quarantine for the shared account.



Clicking on a message will allow you to safely view the body of the email so you can decide which action to take.

### Message Actions:

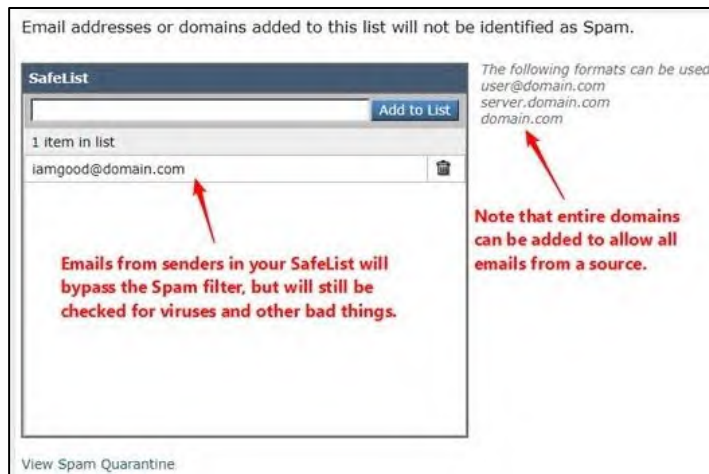
**Release** – Sends email to your Outlook inbox. **Only release emails that you believe are safe!** You can always email **S17** to help determine the validity of an email.

**Release and Add to Safelist** - Sends email to your Outlook inbox and adds senders address to your personal safe senders list.

**Delete** – Deletes email from your spam quarantine (this also happens automatically when the message is 14 days old).

Going to **Options** will allow you to navigate to your **SafeList** or **BlockList**. Shown below is the SafeList. Any entries here are for you only. If you feel a sender's email address should be on the SafeList for the entire Commission please contact **S17**





The BlockList functions in the same manner as the SafeList but blocks emails from the sender instead of allowing.

**If you are unsure whether to block or allow future emails – do nothing!** Future similar emails will likely just end up in the quarantine again and you may be able to make a better-informed decision.

If you want to go back and manage your SafeList and BlockList you will need to find a previous Spam Quarantine Notification email and use the links. Remember that emails in the Spam Quarantine older than 14 days are automatically deleted.