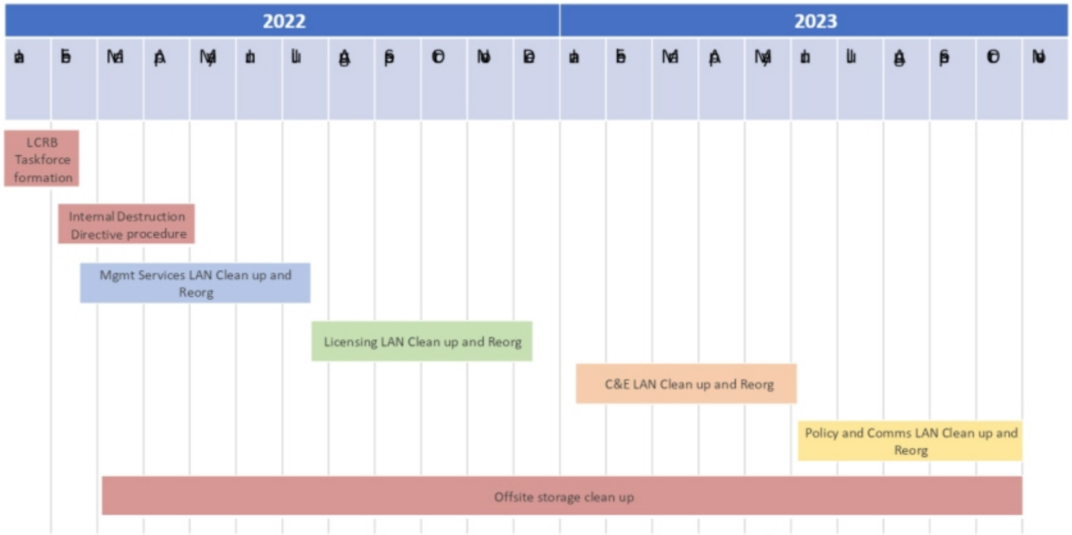
Shared Drive Reorganization & Offsite Storage Cleanup - DRAFT

Updated: January 20, 2022



LCRB Taskforce formation

Internal Destruction Directive procedure

Mgmt Services LAN Clean up and Reorg

Licensing LAN Clean up and Reorg

C&E LAN Clean up and Reorg

Policy and Comms LAN Clean up and Reorg

Offsite storage clean up

Work Streams:	All	Mgmt Services	Licensing	C&E	Policy & Comms

Schedule is subject to change dependent on continual validity of business needs and resource availability

BRITISH COLUMBIA

Liquor and Cannabis
Regulation Branch

2022

Portfolio Charter – Shared Drive Reorganization & Offsite Storage Cleanup

Deleted: ~~Project Charter – Shared Drive Reorganization & Offsite Storage Cleanup~~

2022-03-09 VERSON 5.0

Deleted: ~~2022-01-31 VERSON 3.0~~

Deleted: ~~Project Charter – Shared Drive Reorganization & Offsite Storage Cleanup~~

Deleted: ~~2022-01-31 VERSON 3.0~~

LUKE MAKOWSKI

Portfolio Charter

Portfolio Title	Shared Drive Reorganization & Offsite Storage Cleanup
Start Date	February 15, 2022
Target End Date	November 1, 2023
Project Sponsor	Jennifer Fox
Project Lead	Richard Webster
Project Team Members	Richard Webster, Greg Olaussen, Meghan Glover Higgs, Janeanne Lavassuer, Monica Laube, Staff as assigned
Last Updated	2022-03-09

Deleted: Project

Deleted: Project

Deleted: 1

Deleted: 31

Approvals

Name	Role	Signature	Date
Jennifer Fox	Project Sponsor		

Table of Contents

Deleted:

1.0 Portfolio Overview

Deleted: Project

Form a Records Taskforce to prepare LCRB's electronic and offsite files in anticipation of an eventual amendment to LCRB's ORCS, last updated in 2006, validate compliance to the Information Management Act, and to ensure the LCRB fulfills its long-term records directives and objectives.

2.0 Objectives

The LCRB will form a Records Taskforce, chaired by Management Services FOI Records Officer with membership from each of the working units, to perform a holistic review of LCRB's divisional records practices; prepare the electronic and offsite files in anticipation of an eventual amendment to LCRB's ORCS; and ensure the LCRB fulfills its long-term records maintenance objectives.

This Portfolio requires the completion of various Projects including:

- Formation of the LCRB Records Taskforce
- Review of LCRB's current records practices
- Offsite file clean up and reorganization
- Electronic file clean up and reorganization
- Long-term records maintenance processes

Deleted: roject

Deleted: work streams

Deleted: Coordinate, plan and implement an electronic and o

Deleted: Development and implementation of l

3.0 Scope

3.1 In Scope

The portfolio scope is dependent on continual validation of business needs and priorities as part of the hybrid-agile framework. Some potential improvements identified during the project may be deferred until after the project is complete and will be part of ongoing operational improvements. A repository will be created to track these improvements.

Deleted: project

The following key components have been identified as within scope:

- Formation of the LCRB Records Taskforce
- Analysis of LCRB's current records practices and determine divisional records business needs
- Electronic and offsite file clean up and reorganization in preparation of an eventual amendment to LCRB's ORCS
- Determine long-term records maintenance needs and develop operational procedure
- Routinely review LCRB's records status and assess alignment to the Information Management Act, ARCS/ORCS and LCRB's business needs

Deleted: se

3.2 Out of Scope

The following components are outside of scope:

-

Commented [MLL1]: Any out of scope items? Possibly:

- Analysis and clean up of employees outlook email
- Analysis and clean up of documents stored in Dynamics and Sharepoint

Commented [WRL2R1]: I think this is something that is in scope actually, as many people keep important business related documents in their email instead of where they are supposed to go on the shared drive. This falls under electronic file cleanup, but is just a component of that.

Deleted: se

4.0 Approach

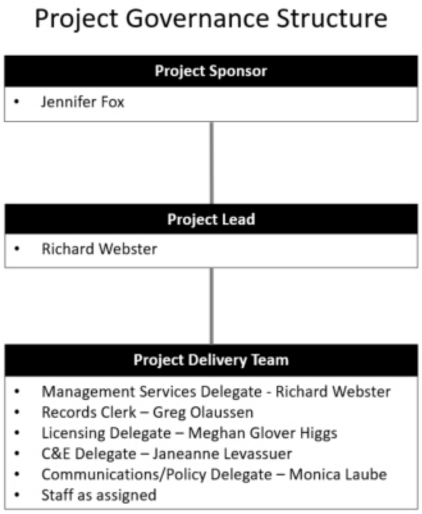
The Records Taskforce, chaired by Management Services FOI Records Officer, will consist of a Records Clerk and 1 member from each of LCRB's working units. Management Services will work with each working unit's representative individually to complete their LAN Restructure and Cleanup. Once respective teams achieve completion, the team's member will remain on the Taskforce to ensure their new LAN structure receives sufficient maintenance. Continued attendance to regular meetings will facilitate additional support to the work unit whose restructure is in progress.

The Project Lead will provide regular updates to the Project Sponsor. Any unresolved issues or changes to scope will need to be reviewed by the Project Sponsor for decision.

The roles of the project team are provided in the Resources section of this document.

4.1 Project Governance

The project governance depicted below will be used to provide oversight and support to the project.



Project Governance Structure

Project Sponsor

- Jennifer Fox

Project Lead

- Richard Webster

Project Delivery Team

- Management Services Delegate - Richard Webster
- Records Clerk – Greg Olaussen
- Licensing Delegate – Meghan Glover Higgs
- C&E Delegate – Janeanne Levassuer
- Communications/Policy Delegate – Monica Laube
- Staff as assigned

4.2 Resources

Role	Primary Responsibility
Project Sponsor	• Establishes project level business objectives and ensures established governance structures and mechanisms are adhered to; • Confirms and approves project scope, and signs off on project plans; • Ensures sufficient funding and operational resources are acquired for the duration of the project; • Promotes project to stakeholders and monitors overall project progress; • Reviews and resolves issues arising from the project; • Reviews and approves change/decision requests;

	• Responsible for final sign-off and success of the project.
Project Lead	• Acts as primary point of contact for communication with the Project Sponsor, including providing project progress updates; • Leads, facilitates, and monitors project activities to meet all deliverables through to successful project completion (within time, budget and quality specifications); • Supports the appropriate engagement of stakeholders; • Motivates and provides leadership to the project team on a day-to-day basis; • Chairs project status meetings and provides guidance to the project team.
Project Delivery Team	• Provides first point of contact for communication with the sub-component project (project stream) team; • Works with Sponsor/Project Lead on delivery dates; • Responsible for delivery of products within project stream including planning, definition of deliverable, resource requirements, completion of tasks, issue resolution, changes and escalation as appropriate; • Collects status from team and communicates to Project Lead on a regular basis as agreed; • Participates and contributes to the delivery of the overall project; and oversees review of deliverables.

5.0 Schedule: Deliverables and Milestones

Proposed Start Date	February 15, 2022

Proposed Close-out Date	November 1, 2023

The detailed portfolio timeline visual is available in Appendix A.

Deleted: project

The major deliverables/milestones are summarized below:

Deliverable/Milestone	Target Completion Date
Formation of LCRB Records Taskforce	February 15, 2022
Management Services LAN clean up and reorg	July 15, 2022
Licensing LAN clean up and reorg	December 15, 2022
C&E LAN clean up and reorg	June 4, 2023
Policy and Communication LAN clean up and reorg	October 31, 2023

Offsite records storage clean up	October 31, 2023

*Deliverables/Milestones and schedule are subject to change dependent on continual validity of business needs and resource availability

5.1 Critical Success Factors

These key components have been identified as critical success factors:

- Executive support and sponsorship
- Support of program area staff and Subject Matter Experts (SME)
- Access to records
- Availability and access to SMEs
- Sufficient readiness in each division to implement change

Deleted: Ministry lead assigned as Project Manager to work in liaison with the developer

6.0 Risks/Challenges and Mitigation

Risk Assessment				
Risk	Probability	Impact	Response Strategy	Residual Risk
Unresponsive program area staff	Med	High	Clearly establish task and milestone owners	Med
Reorganization of the program area	Med	Med	Revaluate business needs and adjust timeline as required	Med
Differing opinions between Exec and staff/ expectation of change	Med	High	Clearly communicate goals & set expectations	Med
Competing priorities may delay targeted completion dates	Med	Med	Establish realistic timelines; obtain Exec support	Med
Change of Taskforce membership	Med	Med	Develop membership succession plan	Med
Hindered or blocked access to records	Low	High	Consensus on access for success in meeting milestones	High
'Scope-Creep' stalling or slowing the project due to additional changes and expectations	Med	Med	Refer to development material to affirm goals, take note of additional expectations for review period.	Med
Missed deadlines	Med	Med	Communicate, adapt, adjust	Med

Commented [MLL6]: Is there a response strategy for this? Possibly: review program structure at regular intervals and assess is LAN reorg is needed

Commented [WRL7R6]: Revaluate business needs and adjust timeline as required

Commented [MLL8R6]: Added

Deleted: e

7.0 Appendix A

7.1 Records Taskforce Details

Commented [MLL9]: May want to update the language in this section to reflect the change of "committee" to "taskforce"

Commented [WRL10R9]: Agree

Records Management Task Force
Shared Drive Reorganization & Offsite Storage Cleanup Plan

Purpose of the Task Force (Committee): To coordinate, plan and implement an electronic and offsite file clean up and reorganization in anticipation of an eventual amendment to LCRB's ORCS, last updated in 2006.

Structure of the Task Force:

- **The Task Force** will consist of 1 member from each of LCRB's working units. Management Services will work with each working unit's representative individually to complete their LAN Restructure/Cleanup. Once respective teams achieve completion, the team's member will remain on the task force to ensure their new LAN structure receives sufficient maintenance. Continued attendance to regular meetings will also facilitate additional support to the work unit whose restructure is in progress.
- **Records Clerk:** Creates the folders, assists teams moving/deleting files, monitoring the ALL STATUS report from Government Records Service (GRS) to identify and fix/report inconsistencies/anomalies in offsite files, assists teams with miscellaneous records tasks, takes the minutes for each meeting, facilitates offsite shipping/receiving.
- **Committee Team Delegates**: Moves files into appropriate folders, destruction of records, consulting with home team for input, communicate important milestones to home team, resolves home team's offsite anomalies with help from the Records Clerk.
- **FOI Records Officer:** Oversees the project, chairs the meetings and provides technical guidance. Provides hands on assistance where required.

Tools:

- One Note will be used to organize the project and each of the task force members will be able to access One Note for reference. One Note will also be promoted as a useful tool for organizing information, as it can be linked to the LAN itself.
- Digital Record Keeping course & Developing organizational excellence should be taken by all members of the committee prior to the first meeting. Members can find the course in the Learning Centre.
- Spreadsheet for tracking each unit's file deletion count in the cleanup and restructure phases.
- Tracking sheet for ORCS planning (What's working/what's not working) will allow for incorporation of cannabis ORCS and update of Liquor ORCS.
- Communication Templates need to be created to be sent out to impacted teams at key intervals though the process (Example: Email to teams to advise of addition of new folders, movement of files ect.)
- All Status Report, which is generated by GRS (for the offsite component)

Meeting Minutes:

- The Records Clerk will maintain meeting minutes for the task force and save the minutes to the LAN in the Records Management folder with a link to One Note.

Meeting Frequency:

- Meetings Will commence Once per month as a group; however, each of the working units will require additional consultation as they work through their LAN restructure.

Structure of Shared Drive clean up/reorg:

- To align as closely with the current LAN structure as possible, we will adopt the "Teams" Structure as outlined in the Digital Record Keeping course. This will allow the project to go ahead without lengthy consultation. Incorporating appropriate classification folders according to ARCS and ORCS does not need consultation, as it is a legislated mandate.
- Records Clerk will create a prototype in H Drive to adopt in phases on each of the teams. A clean slate approach will be needed to address the poor state of the LAN

Phases of Restructure:

- **Preliminary Cleanup Phase -** Transitory records need to be deleted. Gives teams a chance to prepare for the restructure and purge. Also allows for communication to go out to the teams (2 weeks)
- **Re-Org Phase: -** 4 months to complete the job on each team. Create skeleton, move files into the correct classification.
- **Debrief Phase: -** Allows teams to debrief and promote the finished product, make adjustments and plan for the next team.

Sequence of LAN Cleanup timeframes:

1. Management Services Clean up Phase Feb 15-28 2022
2. Management Services Re-Org- March 1 - Jul 1 2022
3. Management Services debrief phase July 1-15 2022
4. Licensing Clean up Phase July 15-31 2022
5. Licensing Re-Org- Aug 1- Dec 1 2022
6. Licensing debrief phase Dec 1 - 15 2022
7. C&E Clean up Phase January 7-21 2023
8. C&E Re-Org- January 21-May 21 2023
9. C&E debrief phase May 21 -Jun 4 2023
10. Policy and Comms Clean up Phase Jun 4- Jun 18 2023
11. Policy and Comms Re-Org Jun 18-Oct 18 2023
12. Policy and Comms debrief phase Oct 18-31 2023

Offsite storage clean up:

- Pull the All-Status Report from GRS on a monthly basis.
- Records Clerk will order materials for each of the program area's
- Records Clerk and Records Officer will provide assistance and seek direction from working units to determine final disposition/coordinate destruction or correct classification.

Internal Destruction Directive (April 2022):

- Develop a process for file destruction including establishing roles.
- Determine final approval route for internal destruction
- Prepare branch communication surrounding change
- Develop tracking sheets for oversight on destroyed files (except transitory or redundant).

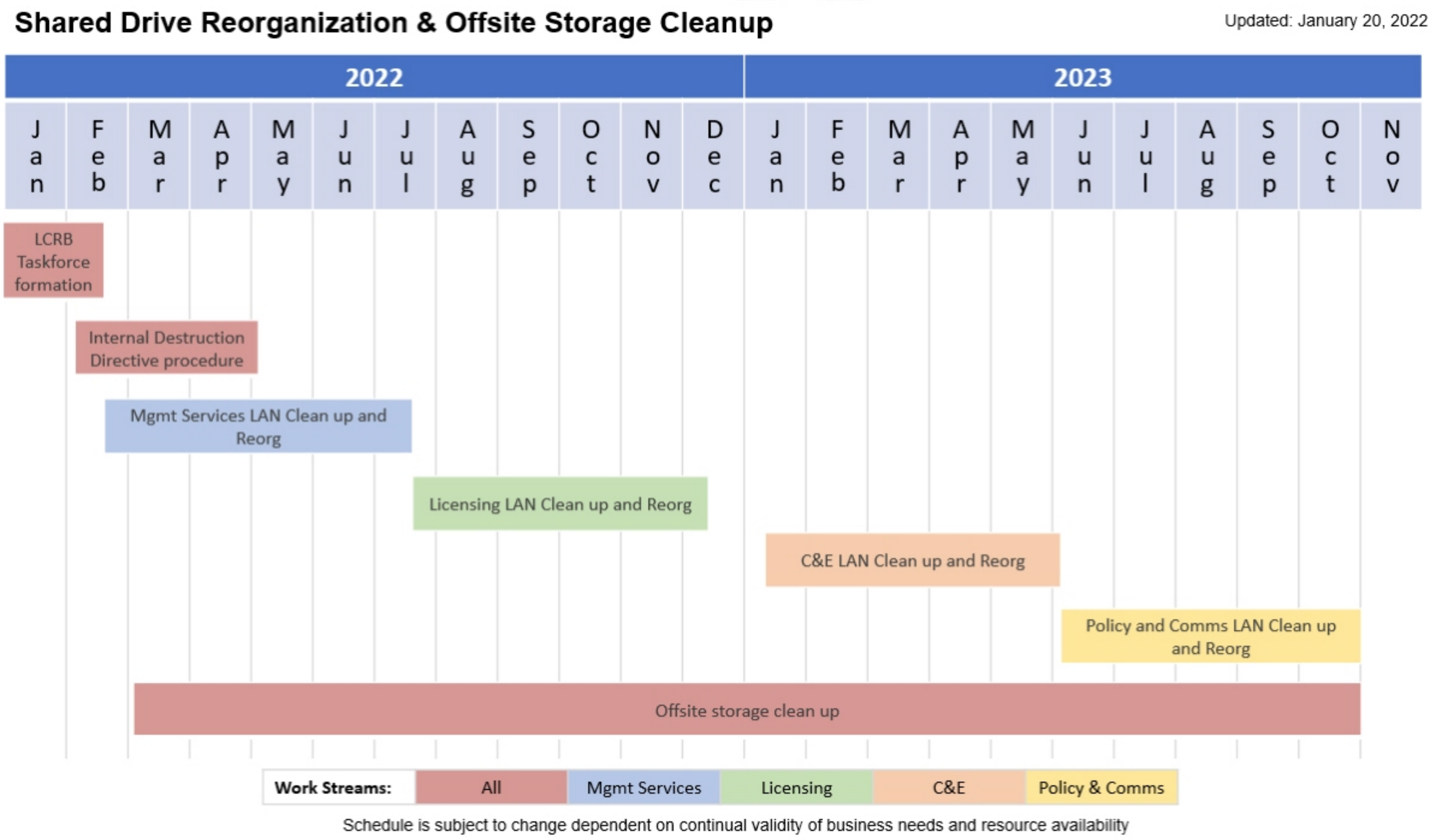
Deleted: Purpose of the Committee: To coordinate, plan and implement an electronic and offsite file clean up and reorganization in anticipation of an eventual amendment to LCRB's ORCS, last updated in 2006.

Structure of the Committee:
The Committee will consist of 1 member from each of LCRB's working units. Management Services will work with each working unit's representative individually to complete their LAN Restructure/Cleanup. Once respective teams achieve completion, the team's member will remain on the committee to ensure their new LAN structure receives sufficient maintenance. Continued attendance to regular meetings will also facilitate additional support to the work unit whose restructure is in progress.
Records Clerk: Creates the folders, assists teams moving/deleting files, monitoring the ALL STATUS report from Government Records Service (GRS) to identify and fix/report inconsistencies/anomalies in offsite files, assists teams with miscellaneous records tasks, takes the minutes for each meeting, facilitates offsite shipping/receiving.
Committee Team Delegates: Moves files into appropriate folders, destruction of records, consulting with home team for input, communicate important milestones to home team, resolves home team's offsite anomalies with help from the Records Clerk.
FOI Records Officer: Oversees the project, chairs the meetings and provides technical guidance. Provides hands on assistance where required.

Tools:
One Note will be used to organize the project and each of the committee members will be able to access One Note for reference. One Note will also be promoted as a useful tool for organizing information, as it can be linked to the LAN itself.
Digital Record Keeping course & Developing organizational excellence should be taken by all members of the committee prior to the first meeting. Members can find the course in the Learning Centre.
Spreadsheet for tracking each unit's file deletion count in the cleanup and restructure phases.
Tracking sheet for ORCS planning (What's working/what's not working) will allow for incorporation of cannabis ORCS and update of Liquor ORCS.
Communication Templates need to be created to be sent out to impacted teams at key intervals though the process (Example: Email to teams to

Deleted:

7.2 Timeline



Shared Drive Reorganization & Offsite Storage Cleanup

Updated: January 20, 2022

Schedule is subject to change dependent on continual validity of business needs and resource availability

2022

BRITISH COLUMBIA Liquor and Cannabis Regulation Branch

Project Charter – Management Services Electronic File Cleanup & Reorganization

2022-03-23 VERSON 2.0

LUKE MAKOWSKI

Project Charter

Project Title	Management Services Electronic File Cleanup & Reorganization
Start Date	February 15, 2022
Target End Date	July 15, 2022
Project Sponsor	Jennifer Fox
Project Lead	Richard Webster
Project Team Members	Richard Webster, Greg Olaussen, Staff as assigned
Last Updated	2022-03-23

Approvals

Name	Role	Signature	Date
Jennifer Fox	Project Sponsor		

Table of Contents

1.0 Project Overview

Prepare Management Services electronic files in anticipation of an eventual amendment to LCRB's ORCS, last updated in 2006, validate compliance to the Information Management Act, and to ensure the LCRB fulfills its long-term records directives and objectives.

2.0 Objectives

Management Services will perform a holistic review of the division's records practices, prepare the electronic files in anticipation of an eventual amendment to LCRB's ORCS; and ensure the LCRB fulfills its long-term records maintenance objectives.

This Project requires the completion of various workstreams including:

- Review of Management Services current records practices
- Electronic files clean up
- Electronic files reorganization
- Document long-term records maintenance process needs

3.0 Scope

3.1 In Scope

The project scope is dependent on continual validation of business needs and priorities as part of the hybrid-agile framework. Some potential improvements identified during the project may be deferred until after the project is complete and will be part of ongoing operational improvements. A repository will be created to track these improvements.

The following key components have been identified as within scope:

- Analysis of management services current records practices and determine divisional records business needs
- Management Services electronic file clean up and reorganization in preparation of an eventual amendment to LCRB's ORCS
- Determine long-term records maintenance needs
- Routinely review LCRB's records status and assess alignment to the Information Management Act, ARCS/ORCS and LCRB's business needs

3.2 Out of Scope

The following components are outside of scope:

- Offsite records clean up and reorganization
- Clean up and reorganization of electronic divisional files outside of Management Service's LAN

Commented [MLL1]: Any out of scope items? Possibly:

- Analysis and clean up of employees outlook email
- Analysis and clean up of documents stored in Dynamics and Sharepoint

Commented [WRL2R1]: I think this is something that is in scope actually, as many people keep important business related documents in their email instead of where they are supposed to go on the shared drive. This falls under electronic file cleanup, but is just a component of that.

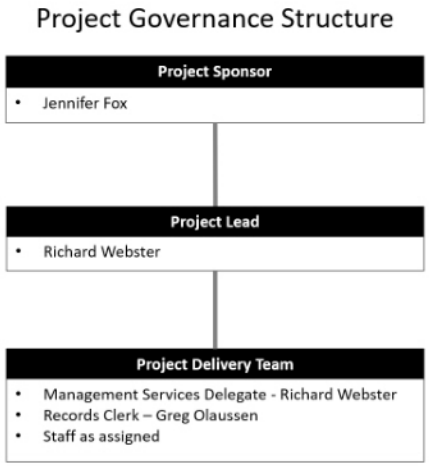
4.0 Approach

The Project Lead will provide regular updates to the Project Sponsor. Any unresolved issues or changes to scope will need to be reviewed by the Project Sponsor for decision.

The roles of the project team are provided in the Resources section of this document.

4.1 Project Governance

The project governance depicted below will be used to provide oversight and support to the project.



Project Governance Structure

Project Sponsor

- Jennifer Fox

Project Lead

- Richard Webster

Project Delivery Team

- Management Services Delegate - Richard Webster
- Records Clerk – Greg Olaussen
- Staff as assigned

4.2 Resources

Role	Primary Responsibility
Project Sponsor	• Establishes project level business objectives and ensures established governance structures and mechanisms are adhered to; • Confirms and approves project scope, and signs off on project plans; • Ensures sufficient funding and operational resources are acquired for the duration of the project; • Promotes project to stakeholders and monitors overall project progress; • Reviews and resolves issues arising from the project; • Reviews and approves change/decision requests; • Responsible for final sign-off and success of the project.
Project Lead	• Acts as primary point of contact for communication with the Project Sponsor, including providing project progress updates; • Leads, facilitates, and monitors project activities to meet all deliverables through to successful project completion (within time, budget and quality specifications); • Supports the appropriate engagement of stakeholders;

	• Motivates and provides leadership to the project team on a day-to-day basis; • Chairs project status meetings and provides guidance to the project team.
Project Delivery Team	• Provides first point of contact for communication with the sub-component project (project stream) team; • Works with Sponsor/Project Lead on delivery dates; • Responsible for delivery of products within project stream including planning, definition of deliverable, resource requirements, completion of tasks, issue resolution, changes and escalation as appropriate; • Collects status from team and communicates to Project Lead on a regular basis as agreed; • Participates and contributes to the delivery of the overall project; and oversees review of deliverables.

5.0 Schedule: Deliverables and Milestones

Proposed Start Date	February 15, 2022

Proposed Close-out Date	July 15, 2022

The detailed project timeline visual is available in Appendix A.

The major deliverables/milestones are summarized below:

Deliverable/Milestone	Target Completion Date
Review of Management Services records practices	
Draft future state LAN structure	
Electronic file inventory	
Electronic file cleanup	
Electronic file reorganization	July 15, 2022
Determine long-term maintenance needs	July 15, 2022

*Deliverables/Milestones and schedule are subject to change dependent on continual validity of business needs and resource availability

Commented [MLL3]: Includes:

- procedure manuals needed
- clean up frequency
- destruction folder review frequency
- etc.

5.1 Critical Success Factors

These key components have been identified as critical success factors:

- Director support and sponsorship
- Support of working unit staff and Subject Matter Experts (SME)
- Access to records
- Availability and access to SMEs

- Sufficient readiness in each working unit to implement change

6.0 Risks/Challenges and Mitigation

Risk Assessment				
Risk	Probability	Impact	Response Strategy	Residual Risk
Unresponsive program area staff	Med	High	Clearly establish task and milestone owners	Med
Reorganization of the program area	Med	Med	Revaluate business needs and adjust timeline as required	Med
Differing opinions between Exec and staff/ expectation of change	Med	High	Clearly communicate goals & set expectations	Med
Competing priorities may delay targeted completion dates	Med	Med	Establish realistic timelines; obtain Exec support	Med
Change of Taskforce membership	Med	Med	Develop membership succession plan	Med
Hindered or blocked access to records	Low	High	Consensus on access for success in meeting milestones	High
'Scope-Creep' stalling or slowing the project due to additional changes and expectations	Med	Med	Refer to development material to affirm goals, take note of additional expectations for review period.	Med
Missed deadlines	Med	Med	Communicate, adapt, adjust	Med

Commented [MLL4]: Is there a response strategy for this? Possibly: review program structure at regular intervals and assess is LAN reorg is needed

Commented [WRL5R4]: Revaluate business needs and adjust timeline as required

Commented [MLL6R4]: Added

7.0 Appendix A

7.1 Records Taskforce Details

Records Management Task Force

Commented [MLL7]: May want to update the language in this section to reflect the change of "committee" to "taskforce"

Commented [WRL8R7]: Agree

Shared Drive Reorganization & Offsite Storage Cleanup Plan

Purpose of the Task Force (Committee): To coordinate, plan and implement an electronic and offsite file clean up and reorganization in anticipation of an eventual amendment to LCRB's ORCS, last updated in 2006.

Structure of the Task Force:

- **The Task Force** will consist of 1 member from each of LCRB's working units. Management Services will work with each working unit's representative individually to complete their LAN Restructure/Cleanup. Once respective teams achieve completion, the team's member will remain on the task force to ensure their new LAN structure receives sufficient maintenance. Continued attendance to regular meetings will also facilitate additional support to the work unit whose restructure is in progress.
- **Records Clerk:** Creates the folders, assists teams moving/deleting files, monitoring the ALL STATUS report from Government Records Service (GRS) to identify and fix/report inconsistencies/anomalies in offsite files, assists teams with miscellaneous records tasks, takes the minutes for each meeting, facilitates offsite shipping/receiving.
- **Committee Team Delegates**: Moves files into appropriate folders, destruction of records, consulting with home team for input, communicate important milestones to home team, resolves home team's offsite anomalies with help from the Records Clerk.
- **FOI Records Officer:** Oversees the project, chairs the meetings and provides technical guidance. Provides hands on assistance where required.

Tools:

- One Note will be used to organize the project and each of the task force members will be able to access One Note for reference. One Note will also be promoted as a useful tool for organizing information, as it can be linked to the LAN itself.
- Digital Record Keeping course & Developing organizational excellence should be taken by all members of the committee prior to the first meeting. Members can find the course in the Learning Centre.
- Spreadsheet for tracking each unit's file deletion count in the cleanup and restructure phases.
- Tracking sheet for ORCS planning (What's working/what's not working) will allow for incorporation of cannabis ORCS and update of Liquor ORCS.
- Communication Templates need to be created to be sent out to impacted teams at key intervals though the process (Example: Email to teams to advise of addition of new folders, movement of files ect.)
- All Status Report, which is generated by GRS (for the offsite component)

Meeting Minutes:

- The Records Clerk will maintain meeting minutes for the task force and save the minutes to the LAN in the Records Management folder with a link to One Note.

Meeting Frequency:

- Meetings Will commence Once per month as a group; however, each of the working units will require additional consultation as they work through their LAN restructure.

Structure of Shared Drive clean up/reorg:

- To align as closely with the current LAN structure as possible, we will adopt the "Teams" Structure as outlined in the Digital Record Keeping course. This will allow the project to go ahead without lengthy consultation. Incorporating appropriate classification folders according to ARCS and ORCS does not need consultation, as it is a legislated mandate.
- Records Clerk will create a prototype in H Drive to adopt in phases on each of the teams. A clean slate approach will be needed to address the poor state of the LAN

Phases of Restructure:

- **Preliminary Cleanup Phase -** Transitory records need to be deleted. Gives teams a chance to prepare for the restructure and purge. Also allows for communication to go out to the teams (2 weeks)
- **Re-Org Phase: -** 4 months to complete the job on each team. Create skeleton, move files into the correct classification.
- **Debrief Phase: -** Allows teams to debrief and promote the finished product, make adjustments and plan for the next team.

Sequence of LAN Cleanup timeframes:

1. Management Services Clean up Phase Feb 15-28 2022
2. Management Services Re-Org- March 1 - Jul 1 2022
3. Management Services debrief phase July 1-15 2022
4. Licensing Clean up Phase July 15-31 2022
5. Licensing Re-Org- Aug 1- Dec 1 2022
6. Licensing debrief phase Dec 1 - 15 2022
7. C&E Clean up Phase January 7-21 2023
8. C&E Re-Org- January 21-May 21 2023
9. C&E debrief phase May 21 -Jun 4 2023
10. Policy and Comms Clean up Phase Jun 4- Jun 18 2023
11. Policy and Comms Re-Org Jun 18-Oct 18 2023
12. Policy and Comms debrief phase Oct 18-31 2023

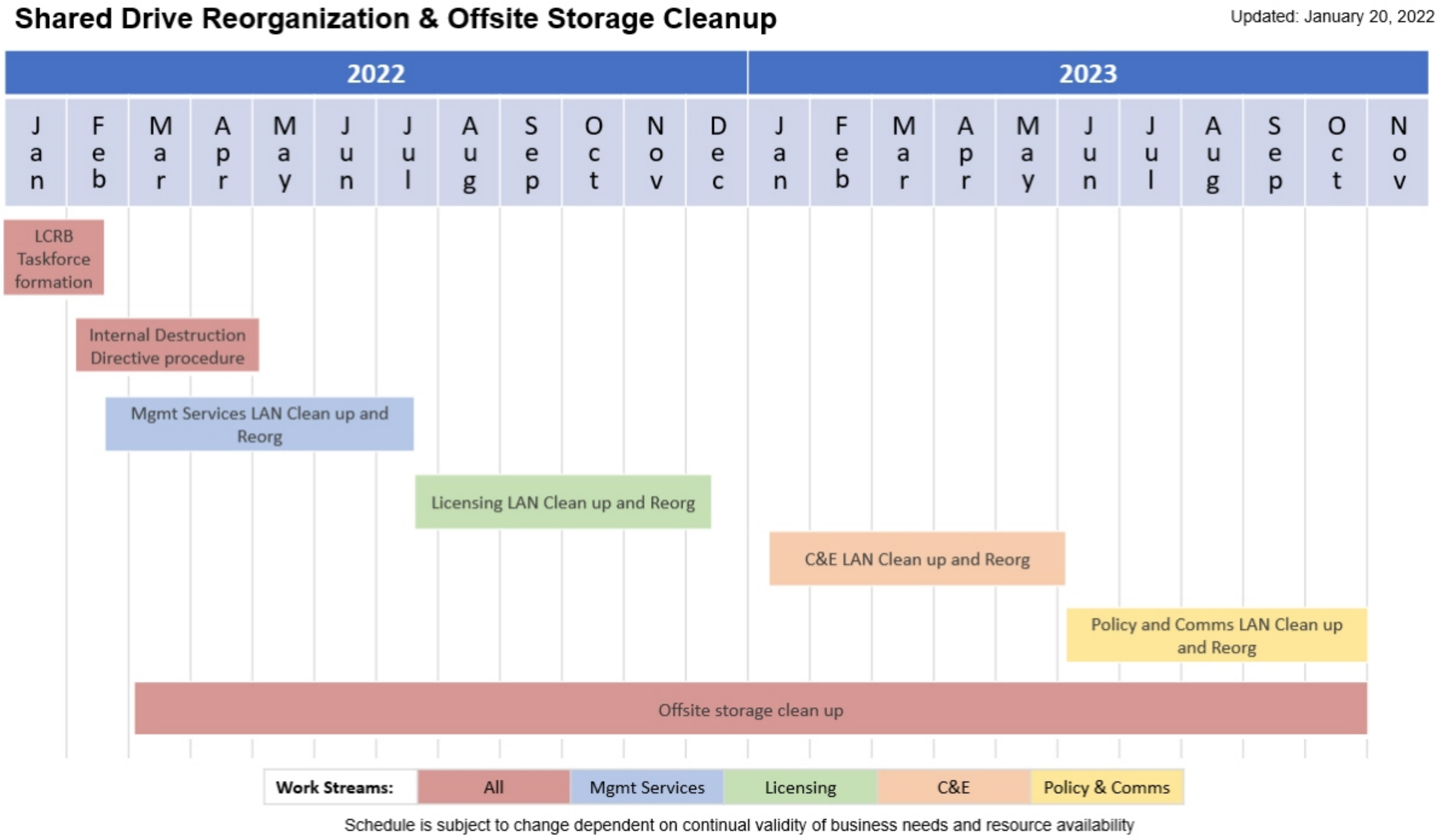
Offsite storage clean up:

- Pull the All-Status Report from GRS on a monthly basis.
- Records Clerk will order materials for each of the program area's
- Records Clerk and Records Officer will provide assistance and seek direction from working units to determine final disposition/coordinate destruction or correct classification.

Internal Destruction Directive (April 2022):

- Develop a process for file destruction including establishing roles.
- Determine final approval route for internal destruction
- Prepare branch communication surrounding change
- Develop tracking sheets for oversight on destroyed files (except transitory or redundant).

7.2 Timeline



Shared Drive Reorganization & Offsite Storage Cleanup

Updated: January 20, 2022

Schedule is subject to change dependent on continual validity of business needs and resource availability

ROTT is detrimental in five important ways. First, it creates excessive storage, infrastructure and maintenance costs. Second, it impairs employees' ability to demonstrate compliance with regulatory guidelines or respond to FOI requests. Third, it impairs employees' ability to quickly access the right information and make data-driven decisions in an agile manner. Fourth, ROTT is often unmanaged and consequently, is vulnerable to data breaches. And fifth, information that is retained beyond its legal retention period poses a liability risk because it can be used against the organization in legal actions or financial audits.

Redundant

Is data that has duplicates stored across multiple locations, perhaps on a different system entirely, perhaps on the system. Intranet systems often contain a large amount of redundant data.

Obsolete

As the name suggests, is information that is no longer accurate or no longer in use. It might be outdated information that has been replaced. It is important to note that not all obsolete files can be arbitrarily deleted. It is only rendered obsolete, if it doesn't fall into the ARCS or ORCS classification. Many government records may appear obsolete but still have a retention schedule.

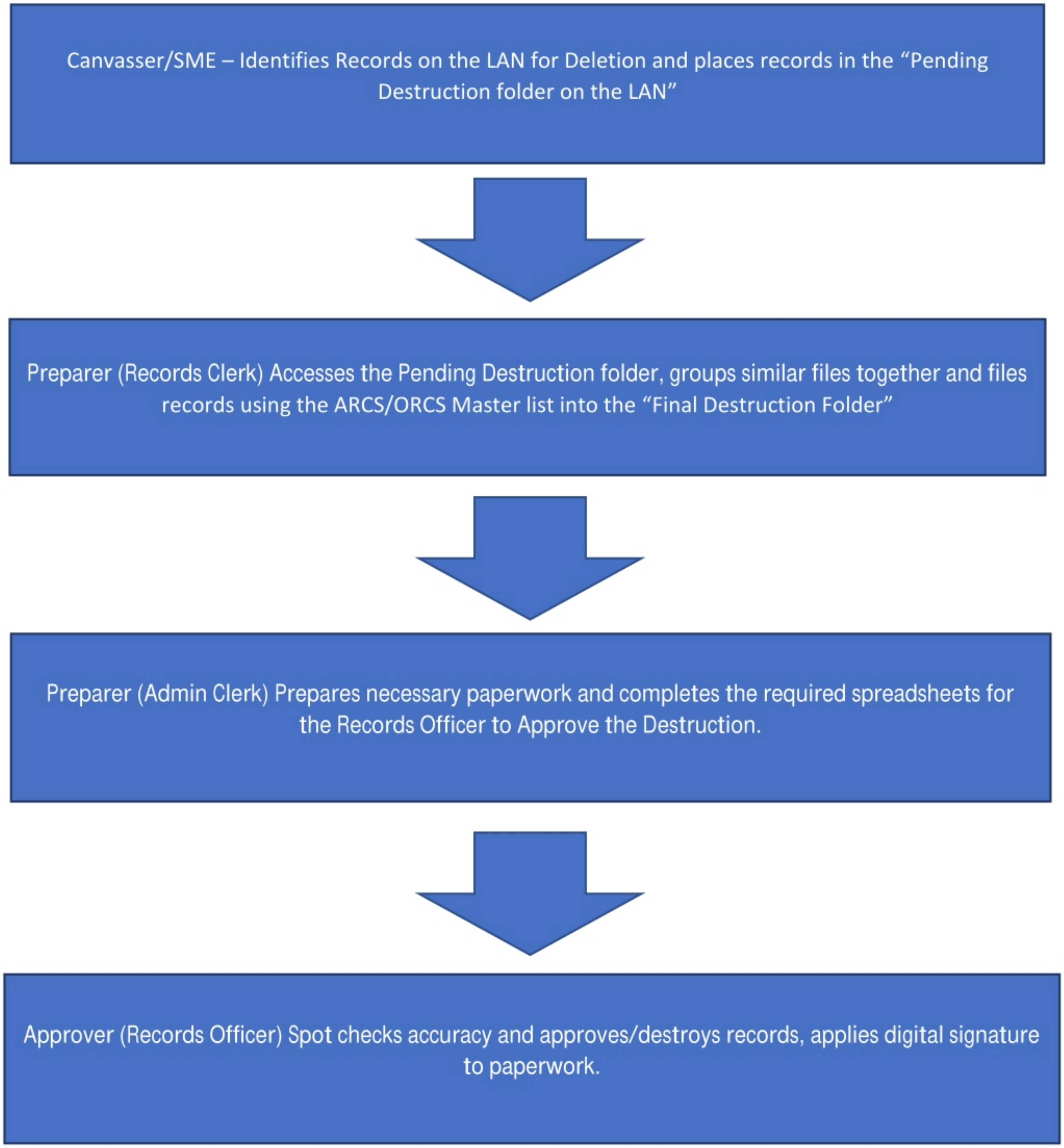
Transitory

Are government records that have short-term use only and do not need to be filed. They are produced or received in the course of routine actions, in the preparation of other records which replace them, or for convenient reference.

Trivial

Is information that isn't necessary to store. It is data that is providing no value to the organization and could be easily removed without any change to the business.

Formal Approval Process



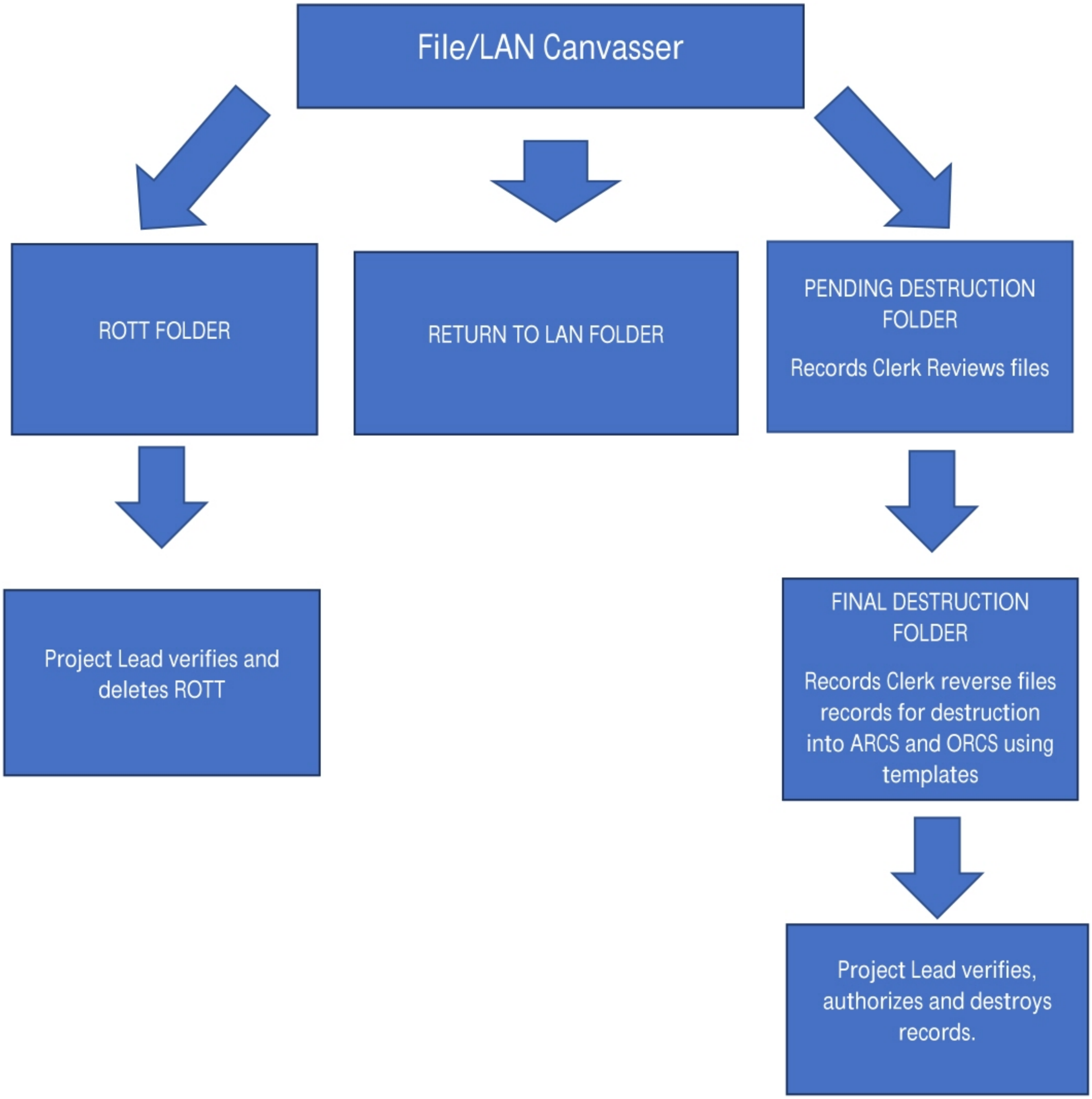
Canvasser/SME – Identifies Records on the LAN for Deletion and places records in the "Pending Destruction folder on the LAN"

Preparer (Records Clerk) Accesses the Pending Destruction folder, groups similar files together and files records using the ARCS/ORCS Master list into the "Final Destruction Folder"

Preparer (Admin Clerk) Prepares necessary paperwork and completes the required spreadsheets for the Records Officer to Approve the Destruction.

Approver (Records Officer) Spot checks accuracy and approves/destroys records, applies digital signature to paperwork.

File Movement Workflow



File/LAN Canvasser

ROTT FOLDER

RETURN TO LAN FOLDER

PENDING DESTRUCTION FOLDER

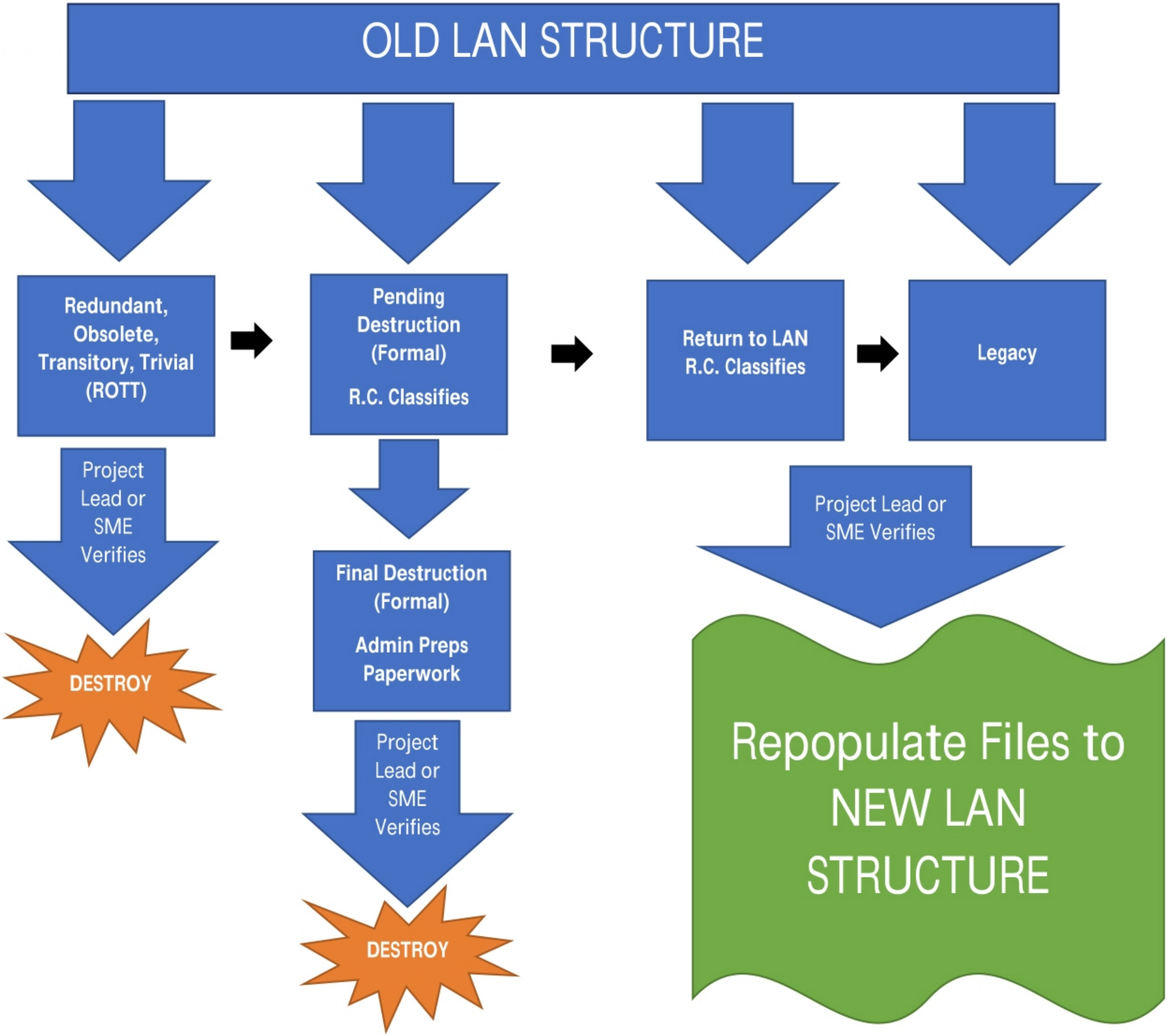
Records Clerk Reviews files

Project Lead verifies and deletes ROTT

FINAL DESTRUCTION FOLDER

Records Clerk reverse files records for destruction into ARCS and ORCS using templates

Project Lead verifies, authorizes and destroys records.



OLD LAN STRUCTURE

Redundant, Obsolete, Transitory, Trivial (ROTT)

Project Lead or SME Verifies

DESTROY

Pending Destruction (Formal)

R.C. Classifies

Final Destruction (Formal)

Admin Preps Paperwork

Project Lead or SME Verifies

DESTROY

Return to LAN R.C. Classifies

Legacy

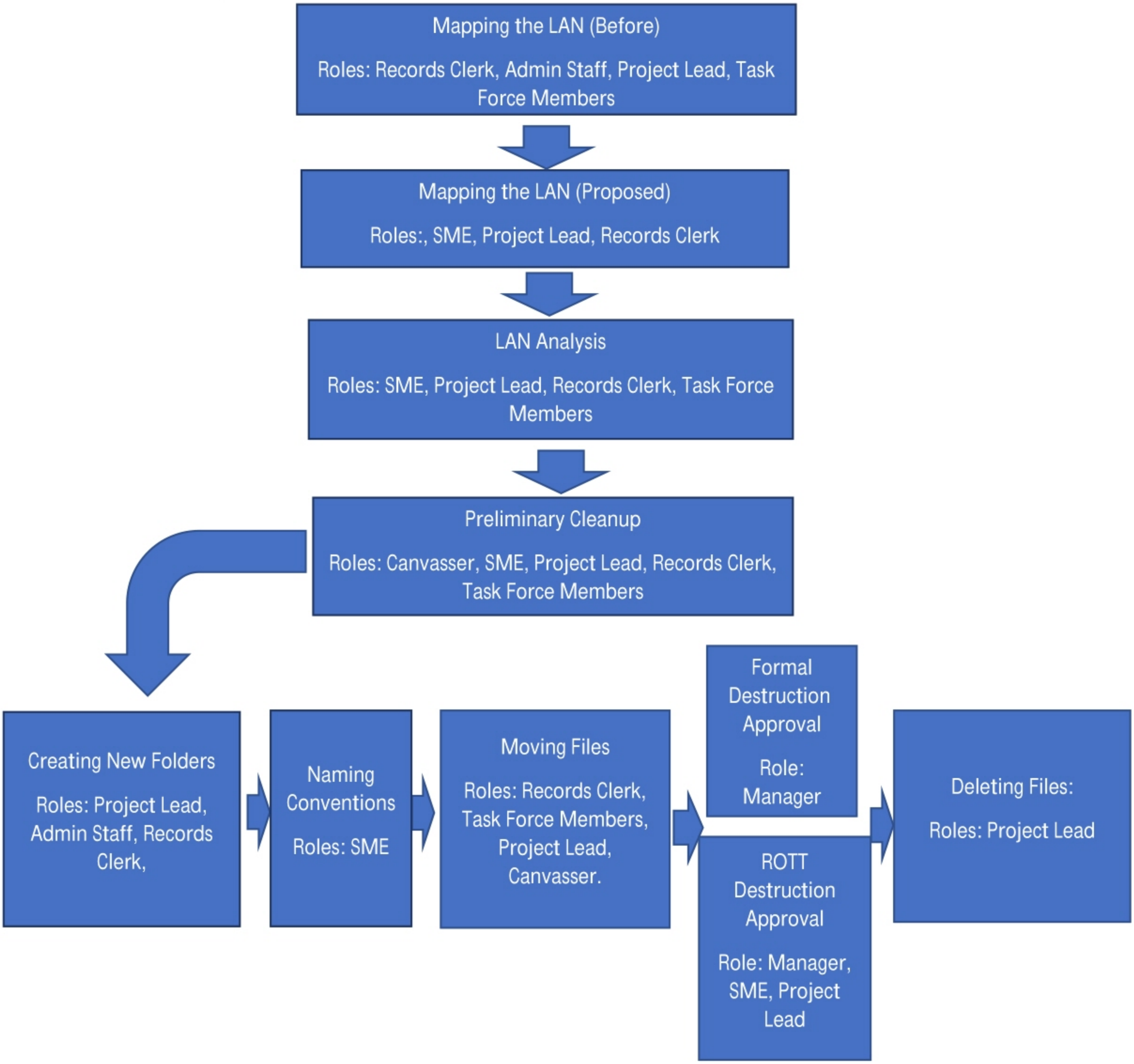
Project Lead or SME Verifies

Repopulate Files to NEW LAN STRUCTURE

ROLES AND RESPONSIBILIES WORKFLOW

The chart below illustrates the order and flow of LAN cleanup; defines each step by role.

- **Subject Matter Expert (SME):** A resource to identify nature and enduring value of LAN content.
- **Canvasser:** Identifies records to keep or delete. A canvasser refers content to the SME.
- **Records Clerk:** Assists as needed, classifies active records and records for destruction
- **Admin Staff:** prepares paperwork for destruction
- **Project Lead:** Assists where needed, moves files, classifies information, provides advice, leads project, creates new LAN structure, provides as much support as required by program area.
- **Task Force Member:** Assists where needed, moves files, classifies info, provides advice, helps leads project, creates new LAN structure, provides as much support as required by program area.
- **Manager/Director:** Set's parameters surrounding roles and responsibilities and allocates resources.



Mapping the LAN (Before)

Roles: Records Clerk, Admin Staff, Project Lead, Task Force Members

Mapping the LAN (Proposed)

Roles:, SME, Project Lead, Records Clerk

LAN Analysis

Roles: SME, Project Lead, Records Clerk, Task Force Members

Preliminary Cleanup

Roles: Canvasser, SME, Project Lead, Records Clerk, Task Force Members

Creating New Folders

Roles: Project Lead, Admin Staff, Records Clerk,

Naming Conventions

Roles: SME

Moving Files

Roles: Records Clerk, Task Force Members, Project Lead, Canvasser.

Formal Destruction Approval

Role: Manager

ROTT Destruction Approval

Role: Manager, SME, Project Lead

Deleting Files:

Roles: Project Lead

Liquor and Cannabis Regulation Branch

RECORDS MANAGEMENT STRATEGY 2022-2027 – LAN CLEAN-UP & RE-ORG

WHY SHOULD WE MAKE RECORDS MANAGEMENT A PRIORITY?

FOI Requests Become Easier to Manage

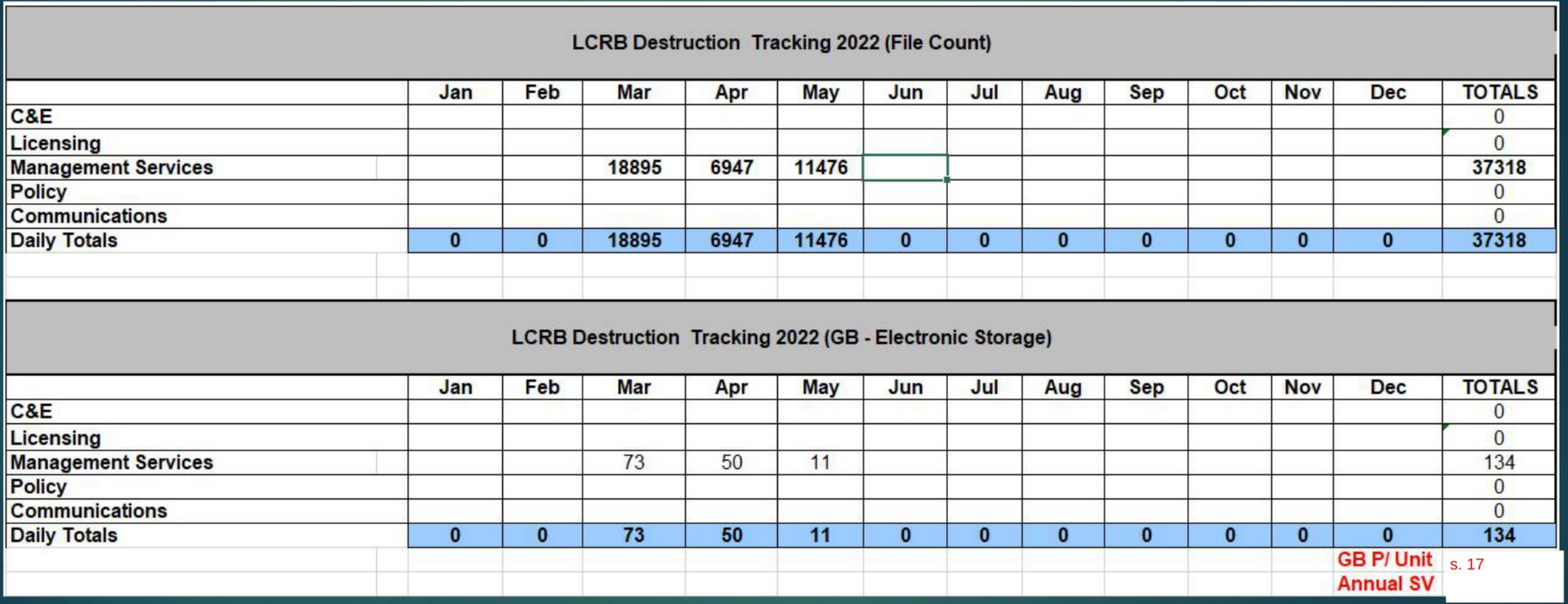
Public Scandal Risk

Chief R.O. 2019 Directive for all Public Bodies to Comply with IMA s.6(1)

Better Transparency

Time Savings

Storage Costs



LCRB Destruction Tracking 2022 (File Count)													
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTALS
C&E													0
Licensing													0
Management Services			18895	6947	11476								37318
Policy													0
Communications													0
Daily Totals	0	0	18895	6947	11476	0	0	0	0	0	0	0	37318

LCRB Destruction Tracking 2022 (GB - Electronic Storage)													
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTALS
C&E													0
Licensing													0
Management Services			73	50	11								134
Policy													0
Communications													0
Daily Totals	0	0	73	50	11	0	0	0	0	0	0	0	134
												GB P/ Unit	s. 17
												Annual SV	

DESTRUCTION AUTHORIZATION RESPONSIBILITIES

GRS Launched service change project April 1, 2022

Ministries are responsible for creating a defensible information destruction model

formal destruction model integration with lan clean up

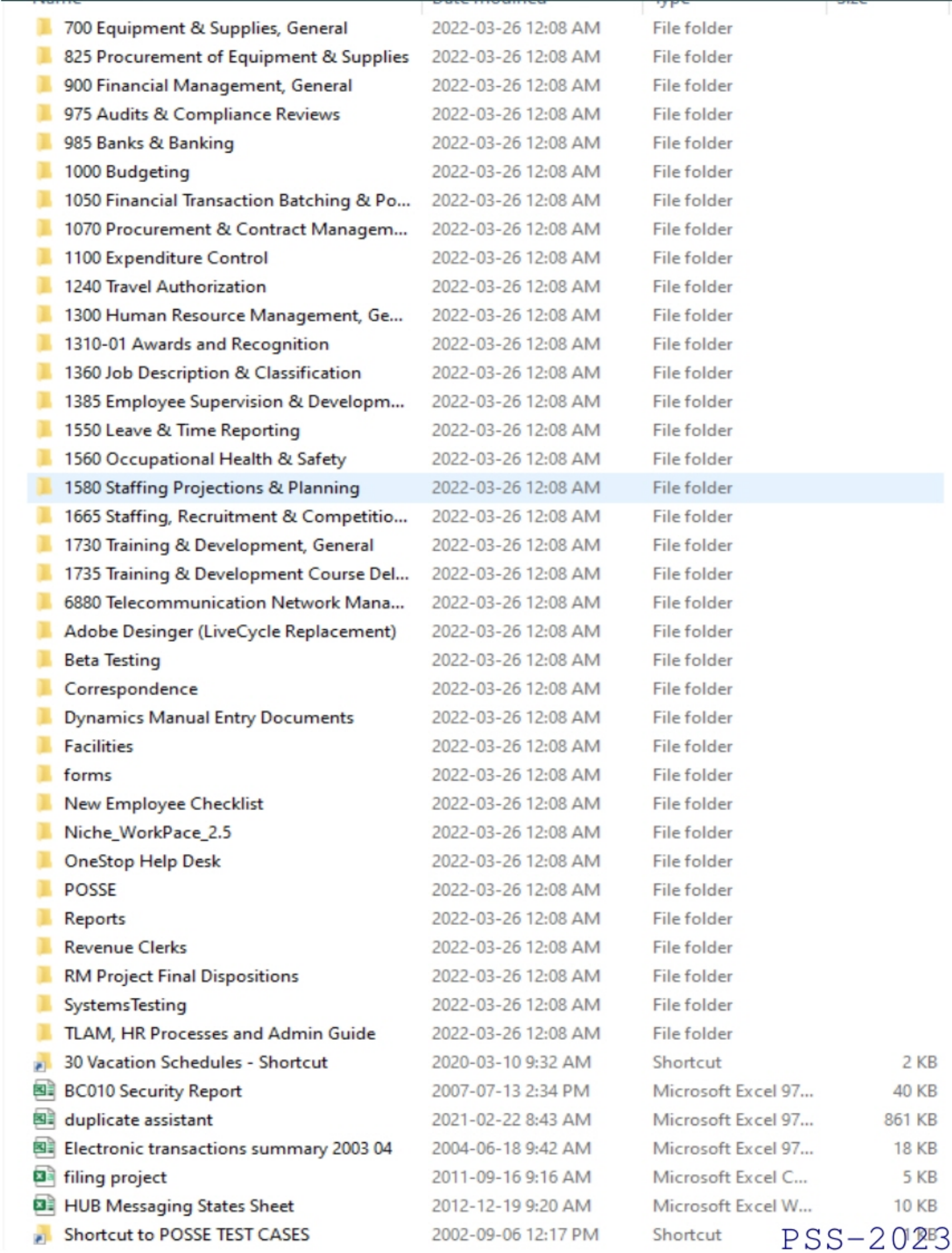
‘TEAMS’ LAN STRUCTURE

- THE TEAMS MODEL AIMS TO MIRROR THE SHARED DRIVE TO THE DIVISIONS IN THE BRANCH
- WITHIN EACH AREA ARE THE ARC OR ORCS THAT ARE RELEVANT TO THE UNIQUE WORK EACH GROUP DOES.
- THE ADMINISTRATION FOLDER IS USED BY ALL THOSE WITH ADMINISTRATIVE RESPONSIBILITIES.
- THE MANAGEMENT FOLDER IS RESTRICTED TO MANAGERIAL STAFF

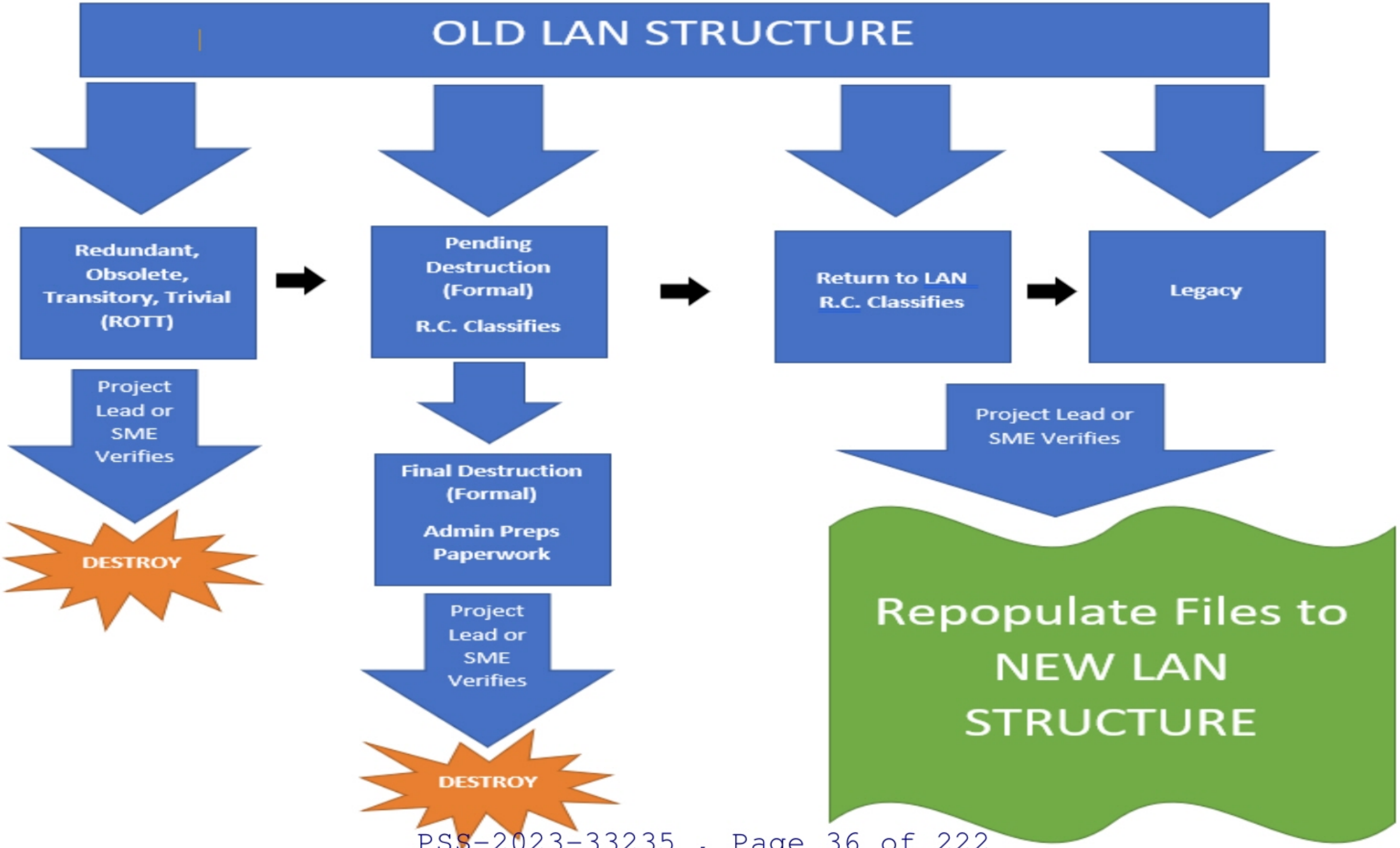
BRITISH COLUMBIA

SHARED DRIVE (LAN) CLEANUP

- IDENTIFY AND REMOVE TRANSITORY & REDUNDANT SOURCE RECORDS
- IDENTIFY AND REMOVE RECORDS MEETING RETENTION SCHEDULE
- CREATE A SHADOW LAN STRUCTURE TO ALIGN WITH ARCS AND ORCS
- ESTABLISH APPROPRIATE NAMING CONVENTIONS
- MIGRATE RECORDS INTO APPROVED BLOCK NUMERIC ARCS/ORCS CLASSIFICATIONS OF PRIMARIES (FUNCTIONS) AND SECONDARIES (ACTIVITIES)



700 Equipment & Supplies, General	2022-03-26 12:08 AM	File folder	
825 Procurement of Equipment & Supplies	2022-03-26 12:08 AM	File folder	
900 Financial Management, General	2022-03-26 12:08 AM	File folder	
975 Audits & Compliance Reviews	2022-03-26 12:08 AM	File folder	
985 Banks & Banking	2022-03-26 12:08 AM	File folder	
1000 Budgeting	2022-03-26 12:08 AM	File folder	
1050 Financial Transaction Batching & Po...	2022-03-26 12:08 AM	File folder	
1070 Procurement & Contract Managem...	2022-03-26 12:08 AM	File folder	
1100 Expenditure Control	2022-03-26 12:08 AM	File folder	
1240 Travel Authorization	2022-03-26 12:08 AM	File folder	
1300 Human Resource Management, Ge...	2022-03-26 12:08 AM	File folder	
1310-01 Awards and Recognition	2022-03-26 12:08 AM	File folder	
1360 Job Description & Classification	2022-03-26 12:08 AM	File folder	
1385 Employee Supervision & Developm...	2022-03-26 12:08 AM	File folder	
1550 Leave & Time Reporting	2022-03-26 12:08 AM	File folder	
1560 Occupational Health & Safety	2022-03-26 12:08 AM	File folder	
1580 Staffing Projections & Planning	2022-03-26 12:08 AM	File folder	
1665 Staffing, Recruitment & Competitio...	2022-03-26 12:08 AM	File folder	
1730 Training & Development, General	2022-03-26 12:08 AM	File folder	
1735 Training & Development Course Del...	2022-03-26 12:08 AM	File folder	
6880 Telecommunication Network Mana...	2022-03-26 12:08 AM	File folder	
Adobe Desinger (LiveCycle Replacement)	2022-03-26 12:08 AM	File folder	
Beta Testing	2022-03-26 12:08 AM	File folder	
Correspondence	2022-03-26 12:08 AM	File folder	
Dynamics Manual Entry Documents	2022-03-26 12:08 AM	File folder	
Facilities	2022-03-26 12:08 AM	File folder	
forms	2022-03-26 12:08 AM	File folder	
New Employee Checklist	2022-03-26 12:08 AM	File folder	
Niche_WorkPace_2.5	2022-03-26 12:08 AM	File folder	
OneStop Help Desk	2022-03-26 12:08 AM	File folder	
POSSE	2022-03-26 12:08 AM	File folder	
Reports	2022-03-26 12:08 AM	File folder	
Revenue Clerks	2022-03-26 12:08 AM	File folder	
RM Project Final Dispositions	2022-03-26 12:08 AM	File folder	
SystemsTesting	2022-03-26 12:08 AM	File folder	
TLAM, HR Processes and Admin Guide	2022-03-26 12:08 AM	File folder	
30 Vacation Schedules - Shortcut	2020-03-10 9:32 AM	Shortcut	2 KB
BC010 Security Report	2007-07-13 2:34 PM	Microsoft Excel 97...	40 KB
duplicate assistant	2021-02-22 8:43 AM	Microsoft Excel 97...	861 KB
Electronic transactions summary 2003 04	2004-06-18 9:42 AM	Microsoft Excel 97...	18 KB
filing project	2011-09-16 9:16 AM	Microsoft Excel C...	5 KB
HUB Messaging States Sheet	2012-12-19 9:20 AM	Microsoft Excel W...	10 KB
Shortcut to POSSE TEST CASES	2002-09-06 12:17 PM	Shortcut	1 KB



OLD LAN STRUCTURE

Redundant, Obsolete, Transitory, Trivial (ROTT)

Project Lead or SME Verifies

DESTROY

Pending Destruction (Formal)

R.C. Classifies

Final Destruction (Formal)

Admin Preps Paperwork

Project Lead or SME Verifies

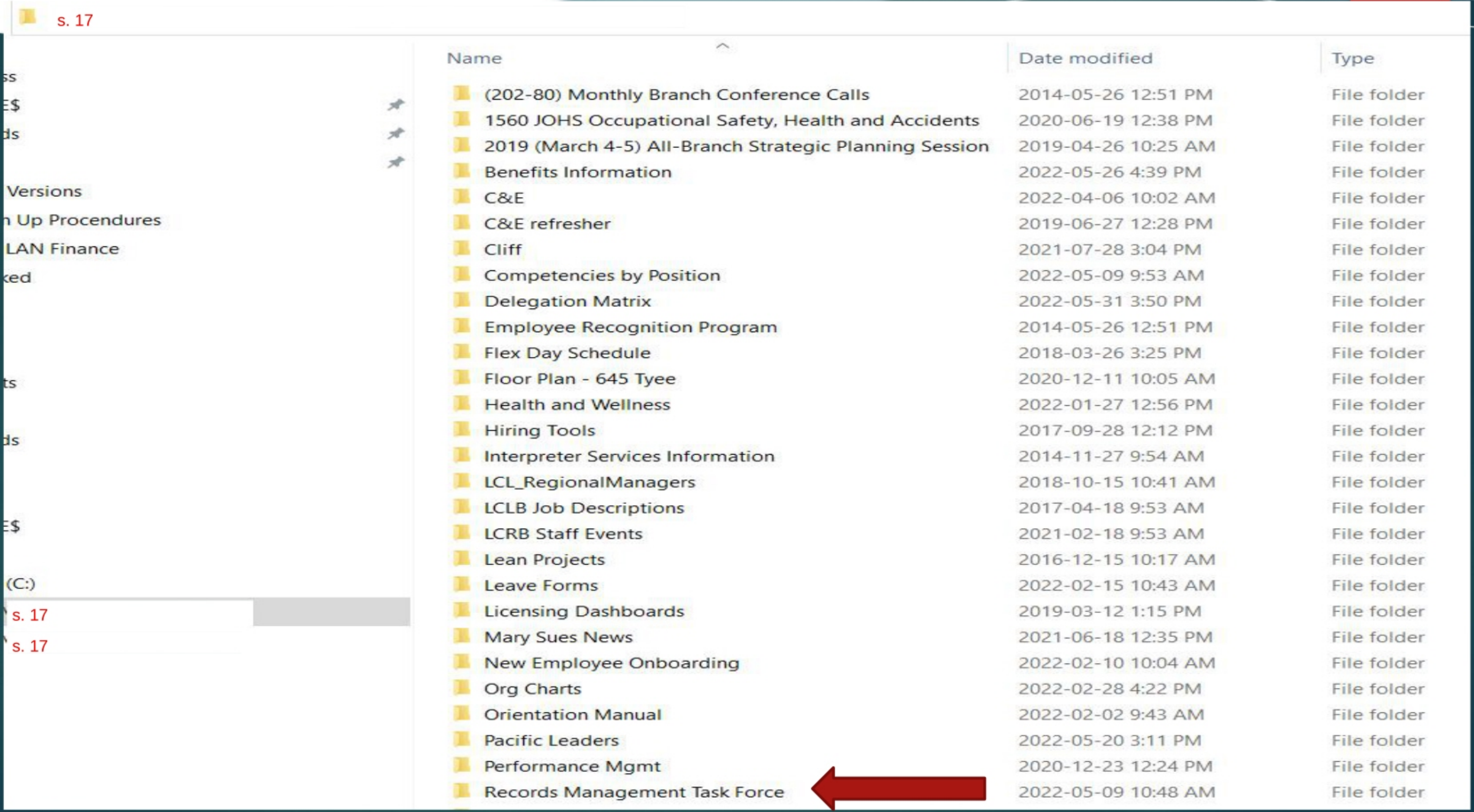
DESTROY

Return to LAN R.C. Classifies

Legacy

Project Lead or SME Verifies

Repopulate Files to NEW LAN STRUCTURE



s. 17

ss
E$
ds
Versions
n Up Procendures
LAN Finance
ked
ts
ds
E$
(C:)
s. 17
s. 17

Name	Date modified	Type
(202-80) Monthly Branch Conference Calls	2014-05-26 12:51 PM	File folder
1560 JOHS Occupational Safety, Health and Accidents	2020-06-19 12:38 PM	File folder
2019 (March 4-5) All-Branch Strategic Planning Session	2019-04-26 10:25 AM	File folder
Benefits Information	2022-05-26 4:39 PM	File folder
C&E	2022-04-06 10:02 AM	File folder
C&E refresher	2019-06-27 12:28 PM	File folder
Cliff	2021-07-28 3:04 PM	File folder
Competencies by Position	2022-05-09 9:53 AM	File folder
Delegation Matrix	2022-05-31 3:50 PM	File folder
Employee Recognition Program	2014-05-26 12:51 PM	File folder
Flex Day Schedule	2018-03-26 3:25 PM	File folder
Floor Plan - 645 Tyee	2020-12-11 10:05 AM	File folder
Health and Wellness	2022-01-27 12:56 PM	File folder
Hiring Tools	2017-09-28 12:12 PM	File folder
Interpreter Services Information	2014-11-27 9:54 AM	File folder
LCL_RegionalManagers	2018-10-15 10:41 AM	File folder
LCLB Job Descriptions	2017-04-18 9:53 AM	File folder
LCRB Staff Events	2021-02-18 9:53 AM	File folder
Lean Projects	2016-12-15 10:17 AM	File folder
Leave Forms	2022-02-15 10:43 AM	File folder
Licensing Dashboards	2019-03-12 1:15 PM	File folder
Mary Sues News	2021-06-18 12:35 PM	File folder
New Employee Onboarding	2022-02-10 10:04 AM	File folder
Org Charts	2022-02-28 4:22 PM	File folder
Orientation Manual	2022-02-02 9:43 AM	File folder
Pacific Leaders	2022-05-20 3:11 PM	File folder
Performance Mgmt	2020-12-23 12:24 PM	File folder
Records Management Task Force	2022-05-09 10:48 AM	File folder

BRITISH COLUMBIA

RISK AND CRITICAL SUCCESS FACTORS

Risk Identification

- unresponsive program area staff
- reorganization of the program area
- change of the membership involved in the project
- unforeseen operational priorities which may put the project on hold
- hindered or blocked access to records
- ‘scope-creep’ that stalls or slows the project because of additional changes or expectations
- missed deadlines on the part of reviewers and the project sponsor

Critical Success Factors

- executive support and sponsorship
- support of program area staff (subject matter experts)
- access to the records (file permissions)
- availability of and access to SMEs
- KPI’s

Destruction Tracker July 2022 (FILES)

Policy & Communications	4	5	6	7	8	11	12	13	14	15	18	19	20	21	22	25	26	27	28	29	30	31	TOTALS
																							0
Policy																185		1813	877				2875
																							0
																							0
																							0
																							0
Daily Totals	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**185**	**0**	**1813**	**877**	**0**	**0**	**0**	**2875**

Destruction Tracker July 2022 (GB)

Policy & Communications	4	5	6	7	8	11	12	13	14	15	18	19	20	21	22	25	26	27	28	29	30	31	TOTALS
																							0
Policy																0.584		1.81	0.83				3.224
																							0
																							0
																							0
																							0
Daily Totals	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1.81**	**1**	**0**	**0**	**0**	**3**

Destruction Tracker July 2022 (FILES)

Policy & Communications	2	3	4	5	8	9	10	11	12	15	16	17	18	19	22	23	24	25	26	29	30	31	TOTALS
																							0
Policy											1174			178	2711							78	4141
																							0
																							0
																							0
																							0
Daily Totals	0	0	0	0	0	0	0	0	0	0	1174	0	0	178	2711	0	0	0	0	0	0	78	4141

s. 17

Destruction Tracker July 2022 (GB)

Policy & Communications	2	3	4	5	8	9	10	11	12	15	16	17	18	19	22	23	24	25	26	29	30	31	TOTALS
																							0
Policy											1.3			0.411	5.21							0.1	7.049
																							0
																							0
																							0
																							0
Daily Totals	0	0	0	0	0	0	0	0	0	0	1	0	0	0.411	5.21	0	0	0	0	0	0	0.1	7

s. 17

Destruction Tracker September 2022 (FILES)

Policy & Communications	1	2	6	7	8	9	12	13	14	15	16	19	20	21	22	23	26	27	28	29	30		TOTALS
																							0
Policy							428			3950	2627												7005
																							0
																							0
																							0
																							0
Daily Totals	**0**	**0**	**0**	**0**	**0**	**0**	**428**	**0**	**0**	**3950**	**2627**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**7005**

s. 17

Destruction Tracker September 2022 (GB)

Policy & Communications	1	2	6	7	8	9	12	13	14	15	16	19	20	21	22	23	26	27	28	29	30		TOTALS
																							0
Policy							0.58			4.76	2.52												7.864
																							0
																							0
																							0
																							0
Daily Totals	**0**	**0**	**0**	**0**	**0**	**0**	**0.58**	**0**	**0**	**4.76**	**3**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**8**

s. 17

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 04/19/2022 **Last Updated:** 04/19/2022

LCRB – Records and Administration- MGT Services

Effective Date: 04/19/2022

Background: For LCRB to gain control of its data, a shared drive cleanup and reorganization must take place. The Destruction Coordinator acts to ensure appropriate paperwork is completed and sees the destruction process through.

Role: Destruction Coordinator Role – Records Officer

- Provides governance, oversight, and administration of the Model
- Acts as a liaison with ministry IM employees (e.g., privacy, security, access, and records) to ensure consistency and collaboration across IM initiatives.
- Liaises with Information Management Branch (IMB) or equivalent, to support coordination of destruction of ministry data.
- Ensures that the necessary resources, tools, and forms are available for ministry program areas to adequately document destructions.
- Defines, documents, and communicates ministry-specific training and knowledge requirements (e.g., destroying government information within a ministry line of business application).
- Ensures that destruction control numbers are issued, and that documentation of approvals is maintained.
- Leads reviews in collaboration with appropriate staff on the effectiveness of the Model and implements improvements, as required.

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 04/19/2022 **Last Updated:** 04/19/2022

LCRB – Records and Administration- MGT Services

Effective Date: 04/19/2022

Background: For LCRB to gain control of its data, a shared drive cleanup and reorganization must take place. The Approver is authorized to permit the destruction of electronic and physical Government Information within the branch's custody and control.

Role: Approver Role: Records Officer, SME, Manager, Director

- Responsible for verifying the destruction is appropriate based on program area knowledge.
- Confirms that records are not needed to meet operational or administrative requirements, related litigation, legal action, requests made under FOIPPA, or investigations that are underway or anticipated.
- Ensure records are only destroyed in accordance with approved information schedules
- Coordinate and ensure appropriate paperwork and spreadsheets are completed to support the defensible destruction of Government Information
- Provides guidance and support to the Preparer and Data Custodians.

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 04/19/2022 **Last Updated:** 04/19/2022

LCRB – Records and Administration- MGT Services

Effective Date: 04/19/2022

Background: For LCRB to gain control of its data, a shared drive cleanup and reorganization must take place. Preparing documents for destruction and filing them in appropriate classification folders will assist the Approver/Coordinator to execute bulk deletions.

Role: Preparer/Data Custodian – Records Clerk, SME

- Responsible for preparing adequate documentation pertaining to government information destructions based on knowledge of records management principles and practices.
- Ensures physical and digital records are only destroyed in accordance with approved information schedules
- Moves electronic files into destruction folders based on classification (ARCS/ORCS) for the Approver and Records Officer to approve/destroy digital information.
- Prepares physical documents for destruction if applicable.
- Oversees the management of data in their program area throughout its lifecycle.
- Meets the requirements of the Data Management Policy and ensures information schedule retentions are applied.

Management Services – Records

Procedure: *Electronic File Cleanup and Reorganization*

Date: 05/02/2022 **Last Updated:** 05/02/2022

LCRB – Records and Administration- MGT Services

Effective Date: 05/02/2022

Background: For LCRB to gain control of its data, a shared drive cleanup and reorganization must take place. Once a canvasser or SME moves irrelevant files (requiring formal destruction approval) from the old LAN structure to the Pending Destruction Folder, preparations must be made to facilitate the file's destruction.

Procedure: Preparing Records for Destruction

Role: Records Clerk

- Access the Pending Destruction Folder to determine contents.
- Utilize the ARCS/ORCS master file list templates located in the LCL_Staffinfo folder, located in the Records Management Task Force sub-folder.
- Copy and paste relevant ARCS/ORCS master template folders into the Final Destruction Folder
- File records in the Pending Destruction Folder into the relevant ARCS/ORCS folder in the Final Destruction folder, grouping similar records together.
- The Files should now be ready for admin staff to complete the appropriate paperwork to complete the destructions. Once the paperwork has been completed, the preparer will move the file into the 'Nuke' folder for final deletion.

Management Services – Records

Procedure: *Electronic File Cleanup and Reorganization*

Date: 04/20/2022 **Last Updated:** 04/20/2022

LCRB – Records and Administration- MGT Services

Effective Date: 04/20/2022

Background: For LCRB to gain control of its data, a shared drive cleanup and reorganization must take place. Preparing paperwork for destruction is an important but heavy administrative endeavor that must be accurate.

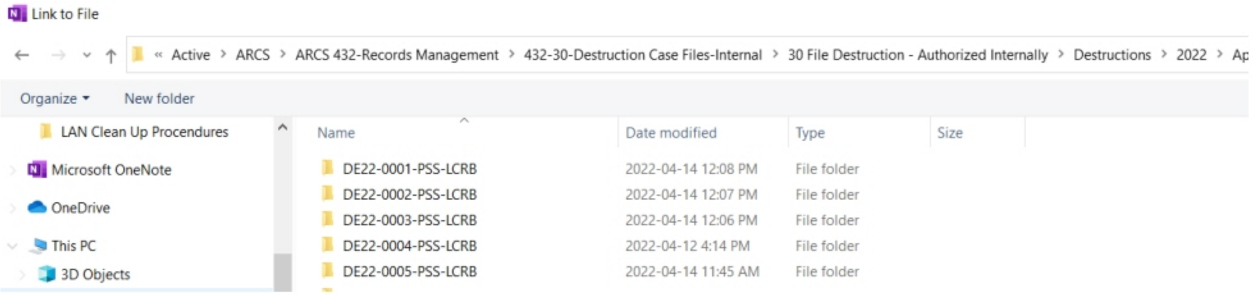
Procedure: Recording Branch Destruction Authorizations

Role: Preparer/Data Custodian – Records Clerk, Records Officer or SME

Step 1: Generate a new Information Destruction Authorization Number (IDA)

- Create a new folder in the Destructions folder to place all the paperwork. The Path to this folder is shown below. The File name for the itemized destruction is the IDA number:

Path: I:\LCL_MgmtServices\FOI Records and Administration\Active\ARCS\ARCS 432-Records Management\432-30-Destruction Case Files-Internal\30 File Destruction - Authorized Internally\Destructions\2022\April


Link to File
« Active › ARCS › ARCS 432-Records Management › 432-30-Destruction Case Files-Internal › 30 File Destruction - Authorized Internally › Destructions › 2022 › Ap
Organize ▾
New folder
LAN Clean Up Procendures
Microsoft OneNote
OneDrive
This PC
3D Objects

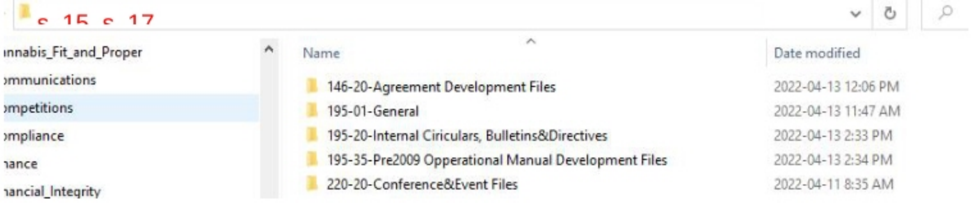
Name	Date modified	Type	Size
DE22-0001-PSS-LCRB	2022-04-14 12:08 PM	File folder	
DE22-0002-PSS-LCRB	2022-04-14 12:07 PM	File folder	
DE22-0003-PSS-LCRB	2022-04-14 12:06 PM	File folder	
DE22-0004-PSS-LCRB	2022-04-12 4:14 PM	File folder	
DE22-0005-PSS-LCRB	2022-04-14 11:45 AM	File folder	

Step 2: Select a destruction list to complete. You can locate a list of files ready for destruction by locating the “Final Destruction” folder in the LAN in the team’s folder you are working on.

Management Services – Records

Procedure: *Electronic File Cleanup and Reorganization*

Example shown below, using Management Services:



s.15 s.17

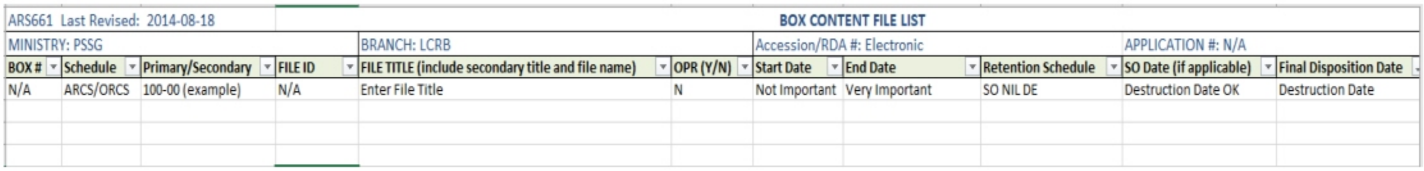
innabis_Fit_and_Proper	
ommunications	
ompetitions	
ompliance	
ance	
ancial_Integrity	

Name	Date modified
146-20-Agreement Development Files	2022-04-13 12:06 PM
195-01-General	2022-04-13 11:47 AM
195-20-Internal Ciriculars, Bulletins&Directives	2022-04-13 2:33 PM
195-35-Pre2009 Opperational Manual Development Files	2022-04-13 2:34 PM
220-20-Conference&Event Files	2022-04-11 8:35 AM

Path: I:\LCL_MgmtServices\RM Project Final Dispositions\Final Destruction

Step 3: Complete the ARS651 Form

- See One Note (Records MGT Task Force/Formal Destruction/Links) to access the ARS 651 template.
- Review the File List Procedure for guidance on exporting data from the LAN to an Excel Spreadsheet.
- Fill in the following fields below:



ARS661 Last Revised: 2014-08-18						BOX CONTENT FILE LIST				
MINISTRY: PSSG				BRANCH: LCRB		Accession/RDA #: Electronic			APPLICATION #: N/A	
BOX #	Schedule	Primary/Secondary	FILE ID	FILE TITLE (include secondary title and file name)	OPR (Y/N)	Start Date	End Date	Retention Schedule	SO Date (if applicable)	Final Disposition Date
N/A	ARCS/ORCS	100-00 (example)	N/A	Enter File Title	N	Not Important	Very Important	SO NIL DE	Destruction Date OK	Destruction Date

- Save the completed form to the newly created IDA file in the destruction folder.
- Rename the file by removing the word template and replace it with the IDA number (DE22-XXXX-PSS-LCRB)
- Since the destruction date is supposed to equal the "start date" of the records series, do not enter any dates, as the Records Officer will complete it upon destruction.

Step 4: Complete the Authorization Form (IDA)

- See One Note (Records MGT Task Force/Formal Destruction/Links) to access the Information Destruction Authorization Form Template.
- Most of the template is already filled out, please change the following fields:
  - Section 3 (Information Identification)
  - Section 4 (Ministry Approver Authorization) except the name of the Approver; the approver will enter his/her name at the time of destruction
- Save the completed form to the newly created IDA file in the destruction folder.

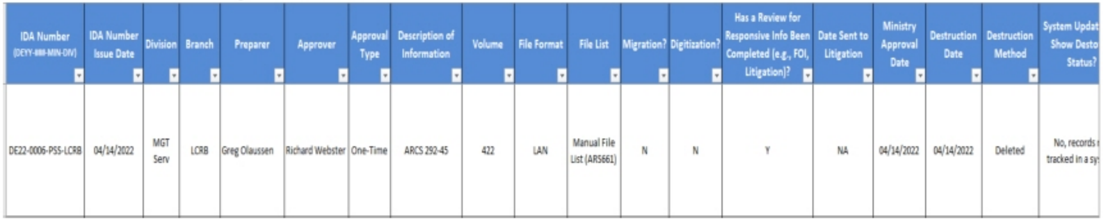
Management Services – Records

Procedure: *Electronic File Cleanup and Reorganization*

- Rename the file by adding the IDA number (DE22-XXXX-PSS-LCRB) to the end of the naming convention.

Step 5: Complete the Destruction Log Spreadsheet with the IDA entry

- See One Note (Records MGT Task Force/Formal Destruction/Links) to access the Destruction Log link.
- Fill in the following fields below:



IDA Number (DEYY-###-MIN-DIV)	IDA Number Issue Date	Division	Branch	Preparer	Approver	Approval Type	Description of Information	Volume	File Format	File List	Migration?	Digitization?	Has a Review for Responsive Info Been Completed (e.g., FOI, Litigation)?	Date Sent to Litigation	Ministry Approval Date	Destruction Date	Destruction Method	System Updat Show Desto Status?
DE22-0006-PSS-LCRB	04/14/2022	MGT Serv	LCRB	Greg Olaussen	Richard Webster	One-Time	ARCS 292-45	422	LAN	Manual File List (ARS661)	N	N	Y	NA	04/14/2022	04/14/2022	Deleted	No, records tracked in a sy

- Generally, there will not be litigation associated with the destruction; however, if there is, the Records Officer will update the spreadsheet accordingly once the list of ongoing litigations are referenced.

Step 6: Move the destruction list to "Nuke Folder" for deletion. You can locate a list of files ready for destruction by locating the "Final Destruction" folder in the LAN in the team's folder. Please remember to add the DE# to the group of records you are destroying by renaming/adding the DE number to the folder before you move it into the "Nuke Folder".

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 03/17/2022 **Last Updated:** 07/18/2022

LCRB – Records and Administration- MGT Services

Effective Date: 03/17/2022

Background: The following document outlines the folders the Records Team will be creating/using inside the LAN to facilitate the clean-up.

Procedure: Folder Description Guide

- Each secondary folder should correspond to an ARCS or ORCS and should also have the following subfolders:
  - A "pending destruction" or (DON'T USE) folder – The pending destruction (Don't Use) folder will contain electronic documents that need to be vetted before moving into the final destruction, legacy or ROTT folders. Task Force reps will need to identify divisional staff (canvassers) authorized to certify the movement of records from the pending to final destruction folders, or seek help from the Records Team.
  - A "Final destruction" folder – Is the last step in a document's life cycle. From this point, the Records Clerk will apply for and create a record of the file's destruction.
    - Inside the final destruction folder, contains a template folder, where the records clerk is able to access empty ARCS and ORCS folders. The Records Clerk can duplicate template folders to bundle files for bulk deletion.
  - A ROTT folder – Files that can be destroyed because it's considered ROTT (Redundant, Obsolete, Transitory, Trivial)
  - A Semi Active Folder – Semi active records have legal, evidential or operational value but are not used on a regular basis. The Semi-Active status is determined by ARCS and ORCS.
  - An Active folder – Contains active/relevant material in regular course of business.
  - A Legacy Folder (optional) - The Legacy Folder is optional and may be required to preserve documents that may add value and have either met their retention or do not have a category in the ARCS or ORCS.

Project: *Electronic File Cleanup and Reorganization*

- A Return to LAN folder (USE FOLDER) – The Return to LAN folder or Use folder is for files that were inappropriately moved to the Pending Destruction folder that need to be returned to the LAN because they are considered Semi-Active or Active. The Return to LAN folder is also a temporary folder that active and semi active files can be moved to while the new LAN structure is set up. Once the setup is complete, team members can move files into their final resting place on the newly restructured LAN by accessing the Return to LAN folder. This folder is for things teams need to keep.
- A For Review Folder (Not Sure Folder) - The For-review folder (not sure folder) is where files are placed to be vetted by either the Records Officer or the SME. The files are reviewed and either moved into the “Return to LAN Folder” or to the various other folders. File Lists can be used to generate discussion for teams if deemed necessary.
- Final Disposition Folders are where SR and FR files are kept. These files have passed their active and semi active schedules and must be kept indefinitely or until an Archivist can do an appraisal on the Selective Retention files.

BRITISH
COLUMBIA

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 03/14/2021 **Last Updated:** 03/14/2021

LCRB – Records and Administration- MGT Services

Effective Date: 03/14/2021

Background: To perform a LAN cleanup, each division will need to know where all their files are located on the share drive. The current LAN structure contains multiple Primary root folders.

Procedure: Map of LAN Before

- Open the excel template named "Excel Template to Map LAN" provided in the Task Force Notebook under your division's dedicated tab.
- Utilize the template to create a high-level overview of your division's LAN structure
  - Fill in your division's existing primary folders
  - Fill in your division's existing secondary folders
- Utilize the note section to describe the content of each secondary folder.
- Review the current mapped overview with divisional stakeholders:
  - Determine if any primary folders require restricted access
  - Review proposed changes and document feedback
- Schedule a meeting with Project Lead and Records Clerk to review
- Begin canvassing the LAN and identify ROTT, Active, Semi Active and records that require destruction.
- Use the mapping document to identify who is working on a particular section of the LAN
- Use the mapping document to flag if your section is "in progress or complete".
- Use the mapping document to identify the SME of the section of the LAN.

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 03/15/2021 **Last Updated:** 04/07/2022

LCRB – Records and Administration- MGT Services

Effective Date: 03/15/2021

Background: For LCRB to gain control of its data, a shared drive cleanup and reorganization must take place. Once a viable and accurate map of the division's LAN has been drafted and approved, it's time to start creating the folders that will mirror the map itself. The folders will be the foundation for the overall structure's permanent location on the LAN.

Procedure: Creating New Folders

Who has authority to create folders? Records Clerk, Project Lead, Task Force Members

- Management Services has created all the ARCS and ORCS folders for each division to use.
    - The files are located in the "all staff info" folder on the LAN but can be accessed VIA the RM Task Force One Note.
    - All folders have a convenient guide embedded within for each ARCS or ORCS
- Copy and paste desired empty folders into an H Drive to match the map created in the LAN mapping excel spreadsheet.
- Follow the instructions below to create the folders in the correct sequence:
    1. Create your division's primary (root) folders
        - Additional folders may be required to restrict access
    2. Create subsequent secondary folders by topic, or teams within each division.
    3. Within each secondary folder should have an Active and a Semi Active folder and Final Disposition folder.
        - Within Active and Semi Active folders will contain ARCS and ORCS to correspond with each category.
        - Within the Final Disposition folder will contain Pending Destruction, Final Destruction, Legacy and ROTT subfolders.

    ❖ Please see folder "Folder Description Guide" for a detailed description of each folder.
- Management Services can assist with this phase depending on divisional operational resources.

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

- Once empty folders have been created, send email to the Project Lead/Records Officer for review.
    - Project Lead/Records Officer will review the work to ensure accuracy and aligns with the standards.
- After consultation with divisional stakeholders, new empty file structures can be placed on the LAN for next steps (moving files)

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 03/21/2021 **Last Updated:** 04/11/2022

LCRB – Records and Administration- MGT Services

Effective Date: 03/21/2021

Background: For LCRB to gain control of its data, a shared drive cleanup and reorganization must take place. After the creation of new folders, the removal of ROTT and records eligible for destruction, the remaining LAN folders should be relevant and can be placed into the corresponding ARCS and ORCS folders.

Procedure: Moving Files After Cleanup

Who has authority to move files into pending or ROTT folders? Records Officer/Project Lead/Task Force members.

- Utilize the ARCS guide linked to the Records Management HUB tab
- Utilize the LCRB ORCS guide (2006)
- Utilize your LAN MAP
- Review the record and determine function
- Move records into corresponding folders by function, accessing the 'return to LAN folder'.
    - Notify your division by email at least 24 hours before you move a group of records into the new location.
    - Advise your division not to go into the folder you are working on during specified timeframes.
    - Notify your division when a section of the LAN movement has been completed
    - Review the newly classified folder(s) with the Project Lead and divisional stakeholders.
- In some instances, you may come across files in your team's folder that should reside in another team's folder.
    - Keep a running list of files in excel spreadsheet to review with SME before moving the files.
    - If cross divisional files reside in another team's folder, move files to the respective team's folders and create a "MISC" folder, so the information can be canvassed by the team's SME. This way the SME can accurately track what their file counts are.

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

- It is imperative that all members of the project team should only move files that are ROTT or have met their retention periods to the Final Disposition folders (Unless it clearly should be for another team's folder, as outlined in the above bullet). If you locate a file that you feel may be out of place, leave it in it's current location, as the working units may need the file to operate. Moving files like this could cause confusion. Only move files to their final destination /return to LAN folder once we establish the new LAN folders and communication has been sent to the impacted working units.
    - An alternative to this would be to add to the name of the file with a clue to where it should belong. For example:
        - File named (Melissa_101) belongs in folder A but you found it in folder B, you could rename it Melissa_101_movetofileb
            - This will flag us to move the file once the re-org takes place.
- ***Depending on divisional resource availability, the Records Team in Management Services is flexible in your team's clean-up and re-org. If there is limited staffing, teams may opt to simply place all the records that have no enduring business value in the 'Pending Destruction Folder' and our records team can move to appropriate final or semi-active destinations.***

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 04/07/2022 **Last Updated:** 04/07/2022

LCRB – Records and Administration- MGT Services

Effective Date: 04/07/2022

Background: For LCRB to gain control of its data, a shared drive cleanup and reorganization must take place. The Final Destruction folder is the final step in the record life cycle. Records flow from the pending destruction folder into the Final Destruction folder

Procedure: Organizing the "Final Destruction Folder"

Role: Records Clerk, Project Lead,

- The Records Clerk accesses the pending destruction folder and identifies groups of records with the same retention/classification schedule to be moved to the Final Destruction folder.
- The Final Destruction Folder contains a subfolder called the 'template folder'. It contains ARCS and ORCS skeleton folders.
- The Records Clerk copies relevant skeleton ARCS and/or ORCS folders from the template folder and posts them to the Final Destruction folder
- The Records Clerk moves bundled files from the Pending Destruction folder into the relevant copied skeleton folders so a bulk deletion can occur.
- The Records Officer will complete the appropriate authorization forms, review and destroy records residing in the Final Destruction folder
- For more information on the formal destruction process, please see the Formal Destruction tab in One Note.

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 03/29/2021 **Last Updated:** 03/29/2021

LCRB – Records and Administration- MGT Services

Effective Date: 03/29/2021

Background: For LCRB to gain control of its data, a shared drive cleanup and reorganization must take place. Files on the LAN that are up for deletion; or need to be formally destroyed, the final act of either deleting or approving the destruction will take place. The "ROTT" folder will be emptied without formal destruction and the "final destruction folder" will be emptied when management approves the destruction of files that have met their retention schedule.

Procedure: Deleting Files and Approving Destruction

Who has the authority to delete files? Project Lead

- Deleting files will generally happen in the ROTT folder. ROTT doesn't need to be formally destroyed and therefore, can be deleted
- Precautions still need to be taken to ensure ROTT is correctly identified and vetted before deletion. This is why the Project lead has the special permission granted to delete the files to ensure nothing has been incorrectly identified.
- Subject Matter Experts and Management can identify ROTT and the Project Lead should always confirm before deleting ROTT
- The Project Lead is tracking the metrics of the project and therefore, it is advised that the project lead deletes the files to ensure appropriate KPI's are being documented correctly.

Who has the authority to Approve files for destruction? Management

- Files meeting their final disposition requirements need to be formally destroyed according to ARCS and ORCS. Once Identified, these files move into the "pending destruction folders".
- Management will access these folders and double check that these files meet the requirements for destruction.
- Management may opt to keep something they deem valuable and place it in the 'legacy folder'.
- Once approved, the Records Clerk can perform the destruction tasks associated with the record.

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 06/10/2022 **Last Updated:** 06/10/2022

LCRB – Records and Administration- MGT Services

Effective Date: 06/10/2022

Background: For LCRB to gain control of its data, a shared drive cleanup and reorganization must take place. When files reside in the Pending or Final Destruction folder, it will be necessary to generate content list of those files from time to time. The following procedure outlines the instances where a file list must be generated.

Procedure: Establishing the New LAN Structure

- Once all files have been moved into the respective 'holding folders', The Records Team will create the skeleton of the new LAN structure with help from the SME's of the respective program area.
- Templates located in the LCL_Staffinfo folder will be used to create the skeleton structure. Each folder has a user guide.
- The Records Team will access the 'Return to LAN folder' and repopulate the new LAN structure with the active and semi active files that need to be retained.
- The Records Team will send communication out to the impacted areas before actions take place to ensure staff are aware of document locations through the process
- The Records Team will create a Map of the LAN using a spreadsheet or a file list to provide a tutorial of the new LAN structure.

Liquor and Cannabis Regulation Branch

2023

Project Charter – Licensing Electronic File Cleanup & Reorganization

2022-12-05 VERSON 1.0

RICHARD WEBSTER

Project Charter

Project Title	Licensing File Cleanup & Reorganization
Start Date	TBD
Target End Date	TBD
Project Sponsor	Josh Huska
Project Lead	Richard Webster
Project Team Members	Richard Webster, Greg Olaussen, Karen Hodgkinson
Last Updated	2022-12-05

Approvals

Name	**Role**	**Signature**	**Date**
Josh Huska or Designate	Project Sponsor		

Table of Contents

1.0 Project Overview

Prepare Licensing's electronic files in anticipation of an eventual amendment to LCRB's ORCS, last updated in 2006, validate compliance to the Information Management Act, and to ensure the LCRB fulfills its long-term records directives and objectives.

2.0 Objectives

Management Services will perform a holistic review of the division's records practices, prepare the electronic files in anticipation of an eventual amendment to LCRB's ORCS; and ensure the LCRB fulfills its long-term records maintenance objectives.

This Project requires the completion of various workstreams including:

- Review of Licensing's current records practices
- Electronic files clean up
- Electronic files reorganization
- Document long-term records maintenance process needs

3.0 Scope

3.1 In Scope

The project scope is dependent on continual validation of business needs and priorities as part of the hybrid-agile framework. Some potential improvements identified during the project may be deferred until after the project is complete and will be part of ongoing operational improvements. A repository will be created to track these improvements (lessons learned).

The following key components have been identified as within scope:

- Analysis of management services current records practices and determine divisional records business needs.
- Electronic file clean up and reorganization in preparation of an eventual amendment to LCRB's ORCS.
- Determine long-term records maintenance needs.
- Routinely review LCRB's records status and assess alignment to the Information Management Act, ARCS/ORCS and LCRB's business needs

3.2 Out of Scope

The following components are outside of scope:

- MS Outlook Cleanup
- SharePoint Cleanup

4.0 Approach

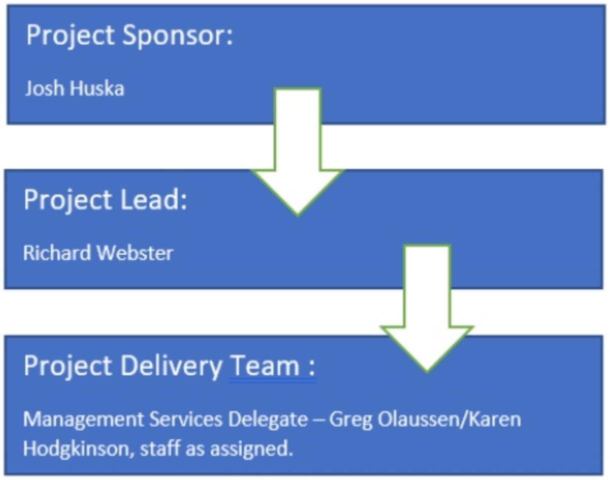
The Project Lead will provide regular updates to the Project Sponsor. Any unresolved issues or changes to scope will need to be reviewed by the Project Sponsor for decision.

The roles of the project team are provided in the Resources section of this document in Appendix A.

4.1 Project Governance

The project governance depicted below will be used to provide oversight and support to the project.

Project Governance Structure


Project Sponsor:
Josh Huska
Project Lead:
Richard Webster
Project Delivery Team :
Management Services Delegate – Greg Olaussen/Karen Hodgkinson, staff as assigned.

4.2 Resources

Role	Primary Responsibility
Project Sponsor	• Establishes project level business objectives and ensures established governance structures and mechanisms are adhered to; • Confirms and approves project scope, and signs off on project plans; • Ensures sufficient funding and operational resources are acquired for the duration of the project; • Promotes project to stakeholders and monitors overall project progress; • Reviews and resolves issues arising from the project; • Reviews and approves change/decision requests; • Responsible for final sign-off and success of the project.
Project Lead	• Acts as primary point of contact for communication with the Project Sponsor, including providing project progress updates; • Leads, facilitates, and monitors project activities to meet all deliverables through to successful project completion (within time, budget and quality specifications); • Supports the appropriate engagement of stakeholders; • Motivates and provides leadership to the project team on a day-to-day basis;

	• Chairs project status meetings and provides guidance to the project team.
Project Delivery Team	• Provides first point of contact for communication with the sub-component project (project stream) team; • Works with Sponsor/Project Lead on delivery dates; • Responsible for delivery of products within project stream including planning, definition of deliverable, resource requirements, completion of tasks, issue resolution, changes and escalation as appropriate; • Collects status from team and communicates to Project Lead on a regular basis as agreed; • Participates and contributes to the delivery of the overall project; and oversees review of deliverables.

5.0 Schedule: Deliverables and Milestones

Proposed Start Date	TBD

Proposed Close-out Date	TBD

The major deliverables/milestones are summarized below:

Deliverable/Milestone	Target Completion Date
Review of Licensing's records practices	TBD
Draft future state LAN structure	TBD
Electronic file inventory	TBD
Electronic file cleanup	TBD
Electronic file reorganization	TBD
Procedure Manuals	TBD

*Deliverables/Milestones and schedule are subject to change dependent on continual validity of business needs and resource availability

5.1 Critical Success Factors

These key components have been identified as critical success factors:

- Director support and sponsorship
- Support of working unit staff and Subject Matter Experts (SME)
- Access to records
- Availability and access to SMEs
- Sufficient readiness in each working unit to implement change

6.0 Risks/Challenges and Mitigation

Risk Assessment				
Risk	Probability	Impact	Response Strategy	Residual Risk
Unresponsive program area staff	Med	High	Clearly establish task and milestone owners	Med
Reorganization of the program area	Med	Med	Revaluate business needs and adjust timeline as required	Med
Differing opinions between Exec and staff/ expectation of change	Med	High	Clearly communicate goals & set expectations	Med
Competing priorities may delay targeted completion dates	Med	Med	Establish realistic timelines; obtain Exec support	Med
Change of Taskforce membership	Med	Med	Develop membership succession plan	Med
Hindered or blocked access to records	Low	High	Consensus on access for success in meeting milestones	High
'Scope-Creep' stalling or slowing the project due to additional changes and expectations	Med	Med	Refer to development material to affirm goals, take note of additional expectations for review period.	Med
Missed deadlines	Med	Med	Communicate, adapt, adjust	Med

7.0 Appendix A

7.1 Records Taskforce Details

Records Management Task Force
Shared Drive Reorganization & Offsite Storage Cleanup Plan

Purpose of the Task Force (Committee): To coordinate, plan and implement an electronic and offsite file clean up and reorganization in anticipation of an eventual amendment to LCRB's ORCS, last updated in 2006.

Structure of the Task Force:

- **The Task Force** will consist of 1 member from each of LCRB's working units. Management Services will work with each working unit's representative individually to complete their LAN Restructure/Cleanup. Once respective teams achieve completion, the team's member will remain on the task force to ensure their new LAN structure receives sufficient maintenance. Continued attendance to regular meetings will also facilitate additional support to the work unit whose restructure is in progress.
- **Records Clerk:** Creates the folders, assists teams moving/deleting files, monitoring the ALL STATUS report from Government Records Service (GRS) to identify and fix/report inconsistencies/anomalies in offsite files, assists teams with miscellaneous records tasks, takes the minutes for each meeting, facilitates offsite shipping/receiving.
- **Committee Team Delegates**: Moves files into appropriate folders, destruction of records, consulting with home team for input, communicate important milestones to home team, resolves home team's offsite anomalies with help from the Records Clerk.
- **FOI Records Officer:** Oversees the project, chairs the meetings and provides technical guidance. Provides hands on assistance where required.

Tools:

- One Note will be used to organize the project and each of the task force members will be able to access One Note for reference. One Note will also be promoted as a useful tool for organizing information, as it can be linked to the LAN itself.
- Digital Record Keeping course & Developing organizational excellence should be taken by all members of the committee prior to the first meeting. Members can find the course in the Learning Centre.
- Spreadsheet for tracking each unit's file deletion count in the cleanup and restructure phases.
- Tracking sheet for ORCS planning (What's working/what's not working) will allow for incorporation of cannabis ORCS and update of Liquor ORCS.
- Communication Templates need to be created to be sent out to impacted teams at key intervals though the process (Example: Email to teams to advise of addition of new folders, movement of files ect.)
- All Status Report, which is generated by GRS (for the offsite component)

Meeting Minutes:

- The Records Clerk will maintain meeting minutes for the task force and save the minutes to the LAN in the Records Management folder with a link to One Note.

Meeting Frequency:

- Meetings Will commence Once per month as a group; however, each of the working units will require additional consultation as they work through their LAN restructure.

Structure of Shared Drive clean up/reorg:

- To align as closely with the current LAN structure as possible, we will adopt the "Teams" Structure as outlined in the Digital Record Keeping course. This will allow the project to go ahead without lengthy consultation. Incorporating appropriate classification folders according to ARCS and ORCS does not need consultation, as it is a legislated mandate.
- Records Clerk will create a prototype in H Drive to adopt in phases on each of the teams. A clean slate approach will be needed to address the poor state of the LAN

Phases of Restructure:

- **Preliminary Cleanup Phase -** Transitory records need to be deleted. Gives teams a chance to prepare for the restructure and purge. Also allows for communication to go out to the teams (2 weeks)
- **Re-Org Phase: -** 4 months to complete the job on each team. Create skeleton, move files into the correct classification.
- **Debrief Phase: -** Allows teams to debrief and promote the finished product, make adjustments and plan for the next team.

Sequence of LAN Cleanup timeframes:

1. C&E Estimate January 30 2023- May 30 2023

Offsite storage clean up:

- Pull the All-Status Report from GRS on a monthly basis.
- Records Clerk will order materials for each of the program area's
- Records Clerk and Records Officer will provide assistance and seek direction from working units to determine final disposition/coordinate destruction or correct classification.

Internal Destruction Directive (April 2022):

- Develop a process for file destruction including establishing roles.
- Determine final approval route for internal destruction
- Prepare branch communication surrounding change
- Develop tracking sheets for oversight on destroyed files (except transitory or redundant)

LCRB LAN Clean-up and Reorganization Project Fact Sheet.

Purpose: To align the branch's records framework with the Information Management Act and the Chief Information Officer's directives.

Quick Facts

- The project launched in April 2022
- Management Services, Policy and Communications have completed the clean-up & Reorganization.
- The project has resulted in the destruction of over 75,000 files, 185 gigs of data, equating to an annual savings s. 17
- LCRB is in a que to receive the assistance of an archivist from Government Records Service to perform an ORCS amendment.
  - last update was in 2006 (doesn't include cannabis). A LAN cleanup and reorganization must take place so we can uncover the gaps in the ORCS for the eventual amendment.
- As of Dec 31, 2022, Government Records Service shifted destruction responsibilities solely to the ministries, therefore requiring an appropriate record keeping system to complete the destructions.

What to Expect

- Files will be moved from their current location to temporary folders while the new structure is built.
- Significant volumes of files will be classified for destruction because the LAN contains records that no longer need to be kept.
- Records on the LAN will be organized into Administrative and Operational Record Classification System (ARCS and ORCS) folders.
- Staff will need to have basic knowledge of ARCS and ORCS so they can file and access their records with ease during the transition and after the reorganization.
- Staff will be required to assist with project related tasks at various points in the timeline. Select staff could be asked to allocate 3-10 hours per week.
- Divisions will need to identify subject matter experts to assist the records team in identifying the purpose and scope of the LAN's contents so appropriate classification and destruction can take place.
- Divisions should be aware that the process can be disruptive and 'bumpy' at times. A level of readiness needs to be accepted before the project begins.
- Timelines will vary depending on complexity, allocation of resources and volumes. The process could take 3-8 months per division.

Steps in the Process

- Mapping the Lan: All root folders and content on the I drive related to your division will need to be mapped prior to file movement using supplied the mapping spreadsheet.

- Identifying Subject Matter Experts (SME's): Using the mapping tool, SME's will need to be identified to speak to the file content as it relates to the division's operational needs.
- Content will need to be classified under ARCS/ORCS and moved to temporary locations.
- Content eligible for destruction will be moved to a destruction folder and await approval for deletion.
- Content identified to be kept will be sorted into Active, Semi Active, Selective and Full retention categories.
- Once all content has been identified, classified and marked for destruction, ARCS and ORCS folders will be created to house the data and the data transfer will take place.

Destruction Tracker Aug - Dec 2022 (FILES)

Communications		TOTALS
		0
Communications		0
ROTT	1388	1388
Formal	11422	11422
		0
		0
Daily Totals	**12810**	**12810**

Destruction Tracker September 2022 (GB)

Communications		TOTALS
		0
Communications		0
ROTT	1.06	1.06
Formal	10.1	10.1
		0
		0
Daily Totals	**11.16**	**11**

Destruction Tracker 2022-2023 (FILES)

Communications		TOTALS
		0
Communications		0
ROTT	1685	1685
Formal	10906	10906
		0
		0
Totals	**12591**	**12591**

Destruction Tracker 2022-2023 (GB)

Communications		TOTALS
		0
Communications		0
ROTT	2.34	2.34
Formal	13.86	13.86
		0
		0
Totals	**16.2**	**16**

Management Services – Records

Procedure: *Electronic File Cleanup and Reorganization*

Date: 03/20/2023   **Last Updated:** 03/20/2023

LCRB – Records and Administration- MGT Services

Effective Date: 03/20/2023

Background: On February 13, 2023, ADM David Hume approved DN Cliff: 638161, which delegated the Manager, Finance, Facilities and Records as Ministry Approver, in the defensible destruction of information at LCRB in accordance with the Information Management Act. The Ministry Approver is the final signing Authority for records that have met their retention schedule as per their approved classifications of ARCS/ORCS. Once approvals have been documented, the records are deleted, shredded or otherwise obliterated.

Procedure: Getting Ministry Approval to Destroy Records

Roles: Destruction Coordinator, Preparer, Approver, Product Owner, Data Custodian

Step 1 Quality Assurance: Data Custodians work in concert with Preparers to get records ready for destruction. By now, records have been identified and all the required documentation has occurred including:

- Information Destruction Authorization Form (IDA)
- Information Destruction Log
- Approval email from the Director (Product Owner) of the relevant division

Before the Ministry Approver receives a request to approve the destruction of records, the FOI Records Officer must review work to ensure accuracy. In the event large volumes of records require approval, a sample QA review is acceptable.

Step 2 Notify the Ministry Approver: The Ministry Approver needs to be notified of the records ready to be destroyed. The FOI Records Officer sends an email to the Ministry Approver. The following needs to be provided to the Ministry Approver Via email:

- The destruction number (or range) in the subject line of the email along with the action being requested Example: DE-2023-01234 or DE-2022-54321 to DE-202254333 FOR APPROVAL
- A path link to the LAN address where the documentation resides.
- A path link to the LAN address where the destruction log resides.
- A confirmation statement that the records are not related to an active FOI request.

Procedure: *Electronic File Cleanup and Reorganization*

- If physical records require destruction, the IDA forms should be provided in the email.
- An template can be used as long as the email contains the pertinent details.
- The FOI Records Officer should file the sent email into a 'pending approval' folder in MS Outlook to keep track of the status.

Step 3 Ministry Approver Review & Approval: The Ministry Approver must review the destruction documentation to determine:

- If Ongoing litigation relates to the records (from an ongoing litigation list from Legal Services Branch)
  - The approver can get a list of ongoing litigation from Nathaniel Carnegie at LSB Nathaniel.Carnegie@gov.bc.ca
- If an active FOI request relates to the records (on the advice of the FOI Records Officer)
- If any risks could arise from the destruction of the records
- Any inconsistencies in documentation (There should be none at this point)

Once the Ministry Approver is satisfied that the destruction criteria is met, an email is sent by reply to the initial email indicating the destruction is approved or denied.

From:	Webster, Richard LCRB:EX
To:	Koehle, Leah LCRB:EX
Cc:	Laube, Monika LCRB:EX
Subject:	Approval of Destructions
Date:	February 16, 2023 10:20:00 AM
Attachments:	image001.png 638161 ADM DBN - Defensible Destruction Model 2023-02-09 FINAL.pdf

Hi Leah

Now that we have largely isolated all the destructions for COMMS, we just need you to review the content to make sure nothing stands out to you as far as risk in deletion. Ongoing litigation and FOI considerations should be made when reviewing, and, content that may have enduring value but has met retention.

Once we get your approval, we have ADM support to get rid of the content. I have attached that BN for your review, so you understand what is happening during the destructions and all the implications

Please review:

I:\LCL_Communications\Z.RECORDS MANAGEMENT PROJECT FOLDERS\FORMAL DESTRUCTION\NUKE FOLDER (PAPERWORK COMPLETE)
I:\LCL_Communications\Z.RECORDS MANAGEMENT PROJECT FOLDERS\OUTLOOK DATA FILES
I:\LCL_Communications\Z.RECORDS MANAGEMENT PROJECT FOLDERS\ROTT

Once reviewed, please provide an email approval for the actual deletion.

Thanks

Richard Webster
Records & FOI Officer |Management Services
Liquor and Cannabis Regulation Branch
Ministry of Public Safety and Solicitor General
Phone: 778-698-5939
Email: Richard.Webster@gov.bc.ca

LCRB LAN Clean-up and Reorganization Project Fact Sheet – Shared Folders .

What's Happening? : LCL_Staffinfo, LCL_GMshared and LCL_Referencedata LAN folders are undergoing a clean up and reorganization. The folder content will be organized differently after the clean-up.

Purpose: To align the branch's records framework with the Information Management Act and the Chief Information Officer's directives. Administrative Classification System (ARCS) and Operational Classification System (ORCS) folders will be implemented.

What to Expect

- Files will be moved from their current locations and organized into categories.
- Significant volumes of files will be classified for destruction because the LAN contains records that no longer need to be kept.
- Records on the LAN will be organized into Administrative and Operational Record Classification System (ARCS and ORCS) folders.
- Staff will need to have basic knowledge of ARCS and ORCS so they can file and access their records with ease during the transition and after the reorganization. The Records Team is there for support and to refer staff to relevant training material.

Steps in the Process

- The records team will contact content owners to consult on file movement and destructions.
- Content will be classified under ARCS/ORCS.
- Content eligible for destruction will be moved to a destruction folder and await approval for deletion.
- Content identified to be kept will be sorted into Active, Semi Active, Selective and Full retention categories.
- Once all content has been identified, classified, and marked for destruction, ARCS and ORCS folders will be created to house the data and the data transfer will take place.

Things to Note:

- There are safety buffers in place to ensure that content is not prematurely deleted. In the unlikely event something deleted is needed, it can be retrieved and restored.
- Some content may be moved to other divisional folders in consultation with relevant divisions.
- Some content (example: The Training folder in LCL_referencedata), will need to be kept intact temporarily because the content is linked to other applications. Once a plan is in place to resolve those limitations, a coordinated approach will take place.

Kick Off – C&E Admin LAN Clean-Up

Richard Webster, FOI Records Officer *05/09/2023*

Purpose: LCRB is in the process of aligning it's physical and electronic records with approved ARCS and ORCS Information Schedules. After a thoughtful and collaborative LAN clean up, the shared drives will look different. These initiatives will pave they way for the development and integration of an updated Operational Records Classification Schedule. The project also aims to ensure records are destroyed according to their information schedules.

Overview of Project Components:

- Project Charter
- Workplan Tracker
- Destruction Tracker
- Mapping Document
- Project Folders
- ARCS/ORCS Folder Templates
- ARCS Website Resource

Quick Facts

- The project launched in April 2022
- Management Services, Policy and Communications have completed the clean-up & Reorganization.
- The project has resulted in the destruction of over 75,000 files, 185 gigs of data, equating to an annual savings of s. 17
- LCRB is in a que to receive the assistance of an archivist from Government Records Service to perform an ORCS amendment.
  - last update was in 2006 (doesn't include cannabis). A LAN cleanup and reorganization must take place so we can uncover the gaps in the ORCS for the eventual amendment.
- As of Dec 31, 2022, Government Records Service shifted destruction responsibilities solely to the ministries, therefore requiring an appropriate record keeping system to complete the destructions.

What to Expect

- Files will be moved from their current location to temporary folders while the new structure is built.
- Significant volumes of files will be classified for destruction because the LAN contains records that no longer need to be kept.
- Records on the LAN will be organized into Administrative and Operational Record Classification System (ARCS and ORCS) folders.

- Staff will need to have basic knowledge of ARCS and ORCS so they can file and access their records with ease during the transition and after the reorganization.
- Staff will be required to assist with project related tasks at various points in the timeline. Select staff could be asked to allocate 3-10 hours per week.
- Divisions will need to identify subject matter experts to assist the records team in identifying the purpose and scope of the LAN's contents so appropriate classification and destruction can take place.
- Divisions should be aware that the process can be disruptive and 'bumpy' at times. A level of readiness needs to be accepted before the project begins.
- Timelines will vary depending on complexity, allocation of resources and volumes. The process could take 3-8 months per division.

Steps in the Process

- Mapping the Lan: All root folders and content on the I drive related to your division will need to be mapped prior to file movement using supplied the mapping spreadsheet.
- Identifying Subject Matter Experts (SME's): Using the mapping tool, SME's will need to be identified to speak to the file content as it relates to the division's operational needs.
- Content will need to be classified under ARCS/ORCS and moved to temporary locations.
- Content eligible for destruction will be moved to a destruction folder and await approval for deletion.
- Content identified to be kept will be sorted into Active, Semi Active, Selective and Full retention categories.
- Once all content has been identified, classified and marked for destruction, ARCS and ORCS folders will be created to house the data and the data transfer will take place.

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Date: 05/18/2023 **Last Updated:** 05/18/2023

LCRB – Records and Administration- MGT Services

Effective Date: 05/18/2023

Background: ROTT consists of Redundant, Obsolete, Transitory, and Trivial files. ROTT doesn't need to be formally destroyed, but it does need to be reviewed and approved for destruction before files can be deleted. It's generally easy to identify trivial and transitory files, but redundant and obsolete files can be difficult to identify as ROTT once they are removed from the context of their original locations. This makes the process of revision unnecessarily difficult, especially if the ROTT folder is being reviewed by a SME who did not participate in the cleanup of the original folder. Sorting ROTT files into general categories during the cleanup process will make it easier for future reviewers to identify which files need further review, and which files can be safely destroyed.

Procedure: Organization of ROTT files within the 'ROTT' folder

- Within each department's ROTT folder, create 3 subfolders: General ROTT, Drafts, and Duplicates. When adding files to the ROTT folder, make sure to place them in the most relevant folder.
- General ROTT: Trivial files, transitory notes, empty folders.
    - These files are easily identified as ROTT even when viewed in isolation.
- 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.
    - Transitory drafts are usually self-evident, but they can be more difficult to confirm as ROTT once removed from their original folder.
- Duplicates: copies of existing records made for purposes of convenience or reference. This is data that has duplicates stored elsewhere on the LAN or in another location such as SharePoint. These transitory duplicates are redundant once they are no longer needed for reference.
    - These are the most difficult to identify once they have been removed from the original folder. When viewed in isolation, most duplicates will look like files that should be kept - many are even titled 'FINAL'.

BRITISH COLUMBIA

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

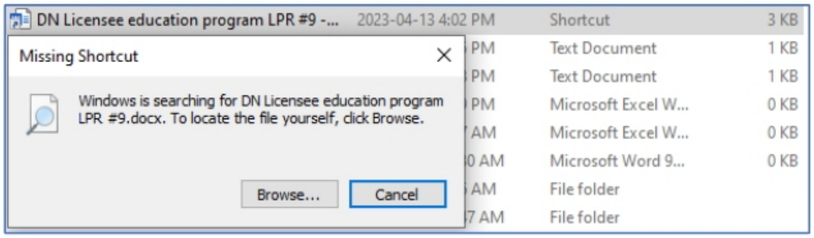
Examples of ROTT

The section below contains examples of the various types of ROTT encountered during the cleanup process.

General ROTT

Transitory systems information, as well as trivial files and transitory notes.

- **Transitory Systems Information**
  Empty folders and shortcuts that are no longer useful can be destroyed as ROTT.

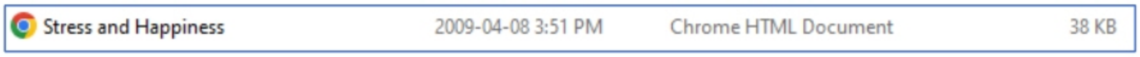


DN Licensee education program LPR #9 -...	2023-04-13 4:02 PM	Shortcut	3 KB
	PM	Text Document	1 KB
	PM	Text Document	1 KB
	PM	Microsoft Excel W...	0 KB
	AM	Microsoft Excel W...	0 KB
	0 AM	Microsoft Word 9...	0 KB
	AM	File folder	
	7 AM	File folder	

Missing Shortcut

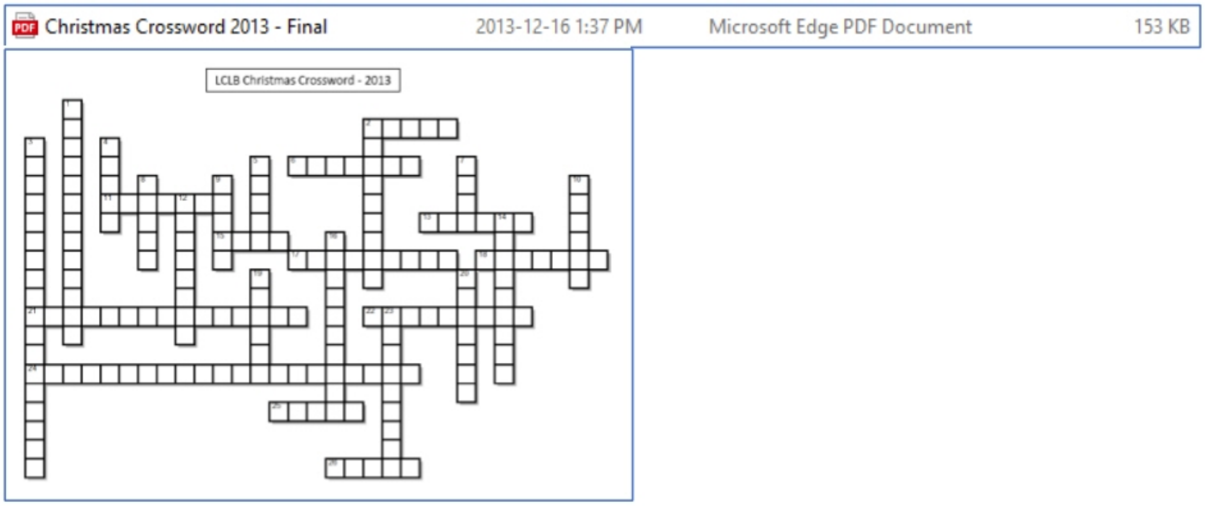
Windows is searching for DN Licensee education program LPR #9.docx. To locate the file yourself, click Browse.

- **Trivial Files**
  The Chrome HTML document shown below is a link to a webpage published by a non-governmental organization. This is **not** a government record and can be destroyed informally as ROTT.



Stress and Happiness	2009-04-08 3:51 PM	Chrome HTML Document	38 KB

This crossword, despite being created by LCRB staff, is not a government record and does not need to be formally destroyed.

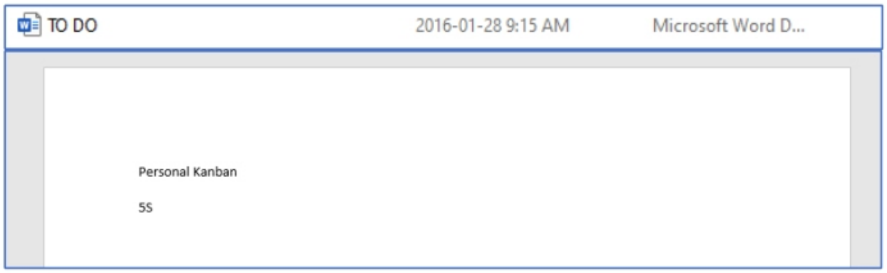


Christmas Crossword 2013 - Final	2013-12-16 1:37 PM	Microsoft Edge PDF Document	153 KB

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

- **Transitory Notes**
  The title and content of the document below indicates that it was used as a temporary and informal organizational tool. This is ROTT.

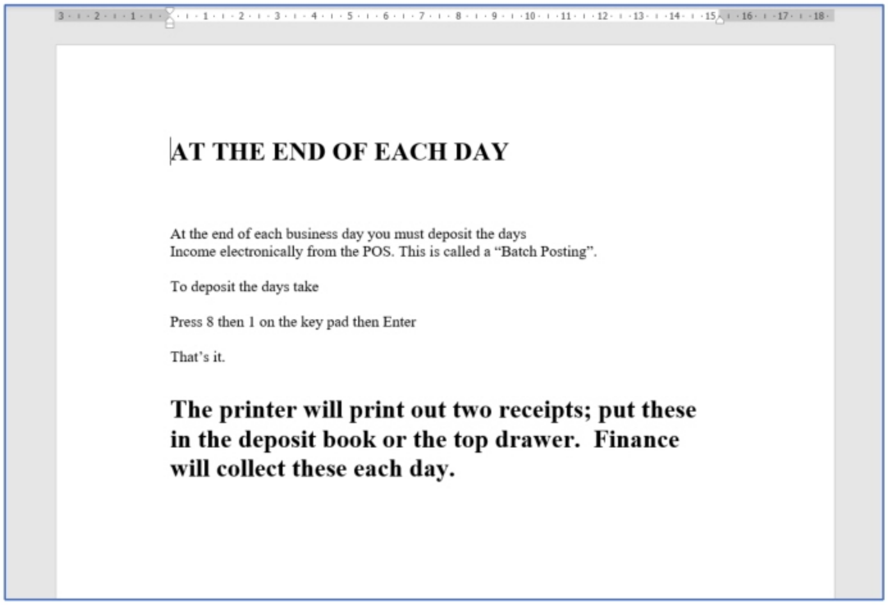


TO DO 2016-01-28 9:15 AM Microsoft Word D...

Personal Kanban

5S

The document below was created as a temporary reference, not a formal record of official procedure, and is considered ROTT.



AT THE END OF EACH DAY

At the end of each business day you must deposit the days
Income electronically from the POS. This is called a "Batch Posting".

To deposit the days take

Press 8 then 1 on the key pad then Enter

That's it.

The printer will print out two receipts; put these in the deposit book or the top drawer. Finance will collect these each day.

Drafts, Rough Notes, and Working Materials

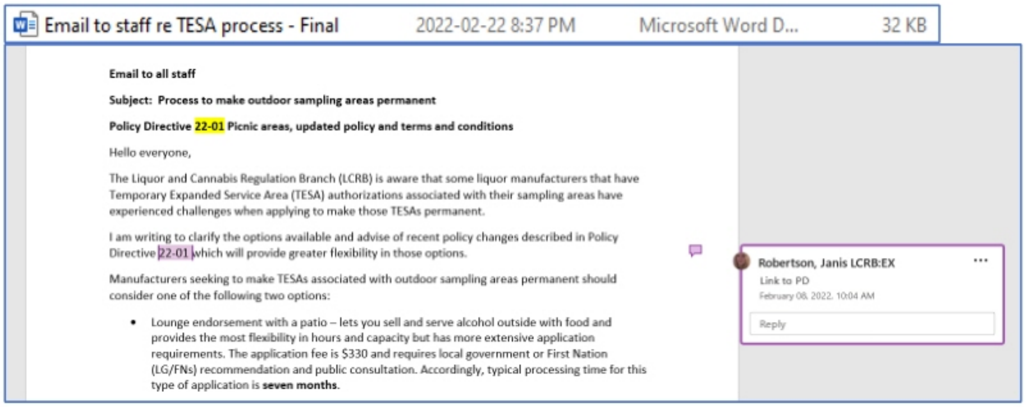
Some drafts provide insight into the evolution of the final document and are needed to understand a key decision-making process. These drafts would be considered records and need to be kept or formally destroyed. However, drafts that do not contain significant comments or substantial changes are considered transitory and can be informally destroyed as ROTT. Similar types of ROTT include rough notes and working materials.

BRITISH
COLUMBIA

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

- **Transitory Drafts, Working Materials, and Rough Notes**
  The document below is an example of a transitory draft because the only edit made to the document is a single comment reminding the author to insert a link into the text. Despite the title of this document, it is not the final version, and the edits it contains are not significant or substantial.



Email to staff re TESA process - Final 2022-02-22 8:37 PM Microsoft Word D... 32 KB

Email to all staff

Subject: Process to make outdoor sampling areas permanent

Policy Directive 22-01 Picnic areas, updated policy and terms and conditions

Hello everyone,

The Liquor and Cannabis Regulation Branch (LCRB) is aware that some liquor manufacturers that have Temporary Expanded Service Area (TESA) authorizations associated with their sampling areas have experienced challenges when applying to make those TESAs permanent.

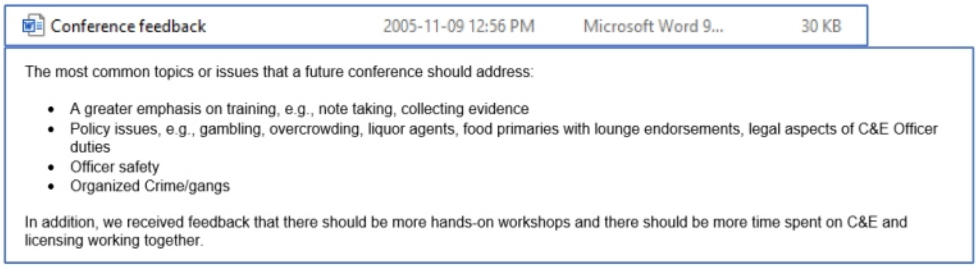
I am writing to clarify the options available and advise of recent policy changes described in Policy Directive 22-01 which will provide greater flexibility in those options.

Manufacturers seeking to make TESAs associated with outdoor sampling areas permanent should consider one of the following two options:

- Lounge endorsement with a patio – lets you sell and serve alcohol outside with food and provides the most flexibility in hours and capacity but has more extensive application requirements. The application fee is $330 and requires local government or First Nation (LG/FNs) recommendation and public consultation. Accordingly, typical processing time for this type of application is **seven months**.

Robertson, Janis LCRB:EX
Link to PD
February 08, 2022, 10:04 AM

The text found in the document below (*Conference feedback*) is exactly duplicated within the final version of another document (*Conference evaluation1*). Therefore, this document would be considered ROTT.



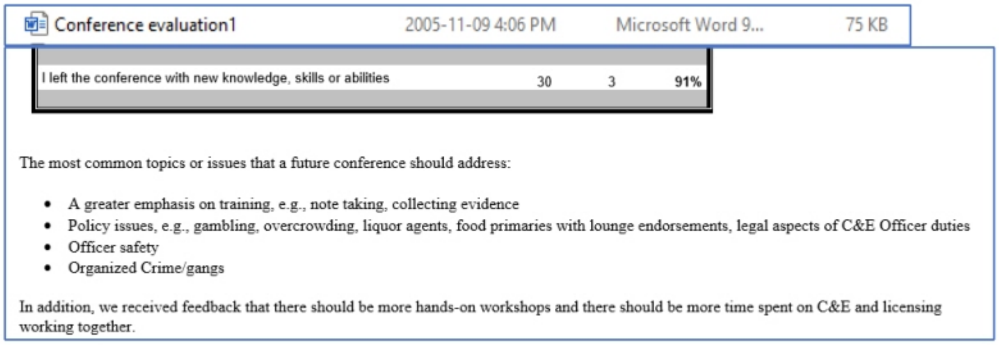
Conference feedback 2005-11-09 12:56 PM Microsoft Word 9... 30 KB

The most common topics or issues that a future conference should address:

- A greater emphasis on training, e.g., note taking, collecting evidence
- Policy issues, e.g., gambling, overcrowding, liquor agents, food primaries with lounge endorsements, legal aspects of C&E Officer duties
- Officer safety
- Organized Crime/gangs

In addition, we received feedback that there should be more hands-on workshops and there should be more time spent on C&E and licensing working together.

The final version of the document (*Conference evaluation1*):



Conference evaluation1 2005-11-09 4:06 PM Microsoft Word 9... 75 KB

I left the conference with new knowledge, skills or abilities	30	3	91%

The most common topics or issues that a future conference should address:

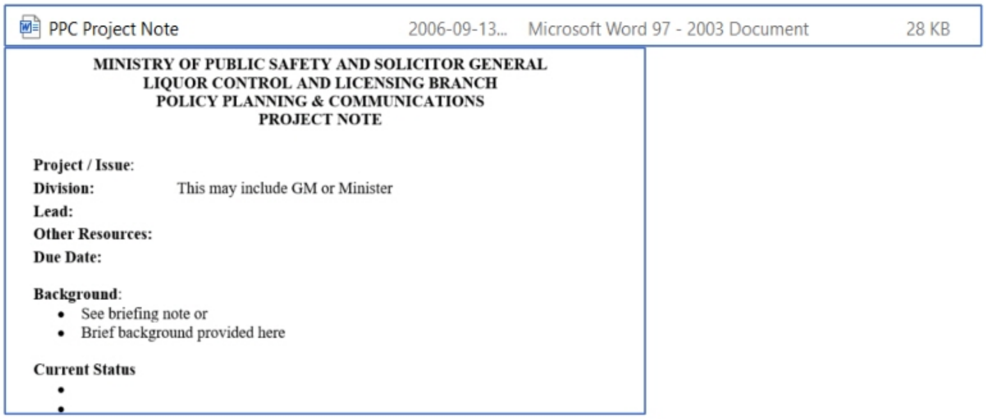
- A greater emphasis on training, e.g., note taking, collecting evidence
- Policy issues, e.g., gambling, overcrowding, liquor agents, food primaries with lounge endorsements, legal aspects of C&E Officer duties
- Officer safety
- Organized Crime/gangs

In addition, we received feedback that there should be more hands-on workshops and there should be more time spent on C&E and licensing working together.

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

The document below is a preliminary outline used in the creation of a Project Note template. It is incomplete and doesn't provide meaningful context to the creation of the final document. This would be ROTT.



PPC Project Note 2006-09-13... Microsoft Word 97 - 2003 Document 28 KB

MINISTRY OF PUBLIC SAFETY AND SOLICITOR GENERAL
LIQUOR CONTROL AND LICENSING BRANCH
POLICY PLANNING & COMMUNICATIONS
PROJECT NOTE

Project / Issue:
Division: This may include GM or Minister
Lead:
Other Resources:
Due Date:

Background:

- See briefing note or
- Brief background provided here

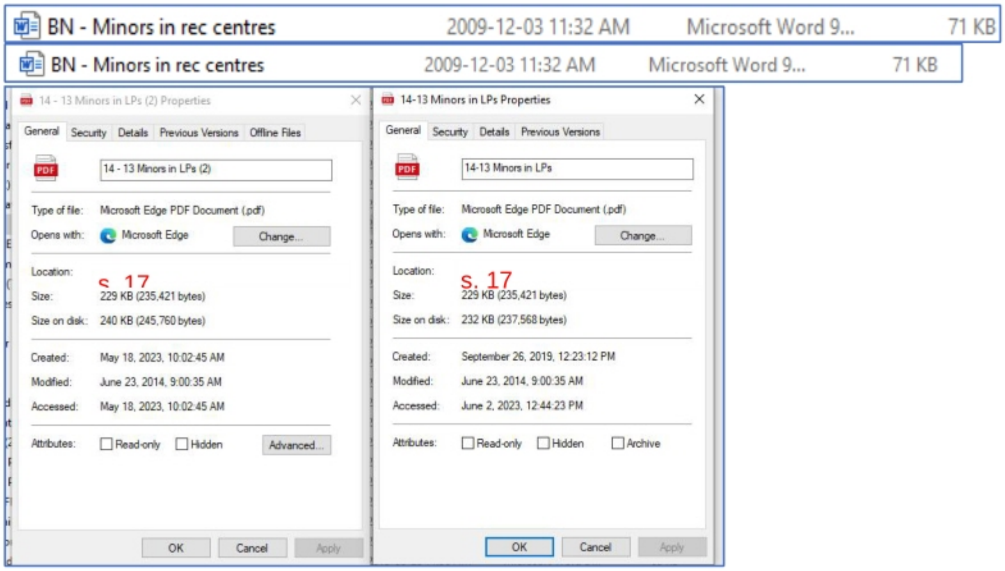
Current Status

-
-

Duplicates

This is data that has duplicates stored elsewhere on the LAN or in another location such as SharePoint. Copies of existing records made for purposes of convenience or reference are considered ROTT.

- The documents below were found in two different locations within the LAN. Looking at the file properties for each of the documents, we can clearly see that these are duplicate files and can destroy one copy as ROTT.



BN - Minors in rec centres 2009-12-03 11:32 AM Microsoft Word 9... 71 KB

BN - Minors in rec centres 2009-12-03 11:32 AM Microsoft Word 9... 71 KB

14 - 13 Minors in LPs (2) Properties

14 - 13 Minors in LPs (2)

Type of file: Microsoft Edge PDF Document (.pdf)
Opens with: Microsoft Edge
Location: s. 17
Size: 229 KB (235,421 bytes)
Size on disk: 240 KB (245,760 bytes)
Created: May 18, 2023, 10:02:45 AM
Modified: June 23, 2014, 9:00:35 AM
Accessed: May 18, 2023, 10:02:45 AM
Attributes: □ Read-only □ Hidden

14-13 Minors in LPs Properties

14-13 Minors in LPs

Type of file: Microsoft Edge PDF Document (.pdf)
Opens with: Microsoft Edge
Location: s. 17
Size: 229 KB (235,421 bytes)
Size on disk: 232 KB (237,568 bytes)
Created: September 26, 2019, 12:23:12 PM
Modified: June 23, 2014, 9:00:35 AM
Accessed: June 2, 2023, 12:44:23 PM
Attributes: □ Read-only □ Hidden □ Archive

BRITISH COLUMBIA

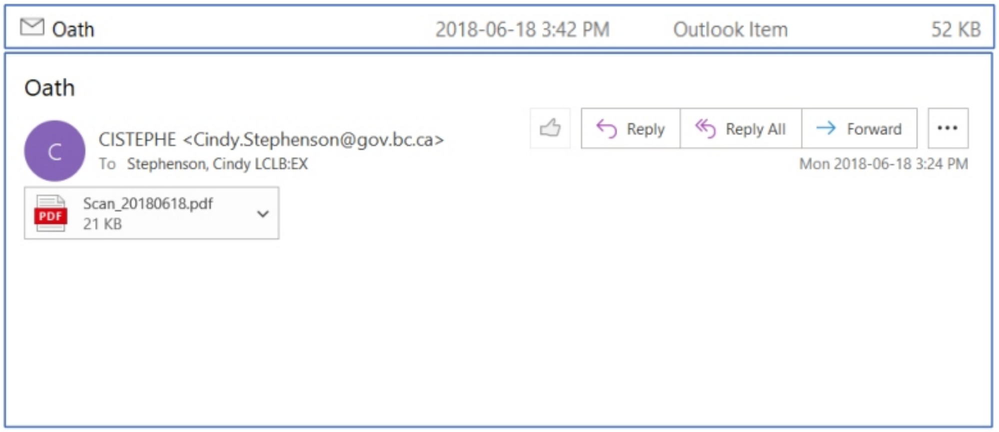
Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Transitory Messages

Many emails are considered transitory and do not need to be kept. Transitory messages are only needed for short-term reference and do not document substantial actions or decisions.

- This email contains an attachment, but there is no text in the body of the email itself. The attachment **would** be considered a record, but the email itself adds no meaningful context to the attachment and would therefore be considered ROTT.



Oath 2018-06-18 3:42 PM Outlook Item 52 KB

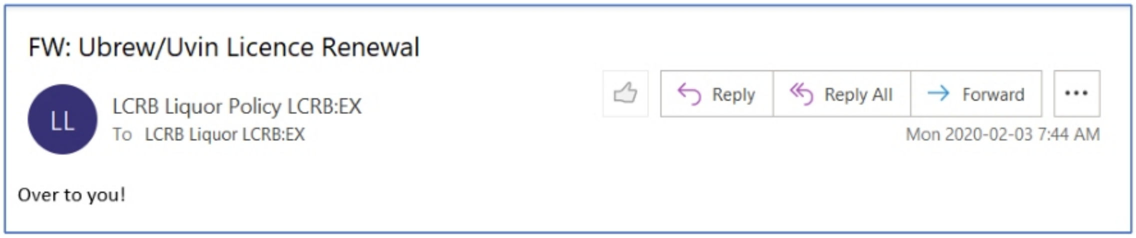
Oath

CISTEPHE <Cindy.Stephenson@gov.bc.ca>
To Stephenson, Cindy LCLB:EX

Mon 2018-06-18 3:24 PM

Scan_20180618.pdf
21 KB

The emails below were saved to the LAN for several years. However, because they only indicate that an incoming email was forwarded to the correct department for processing, these are considered transitory messages and do not need to be treated as official government records.

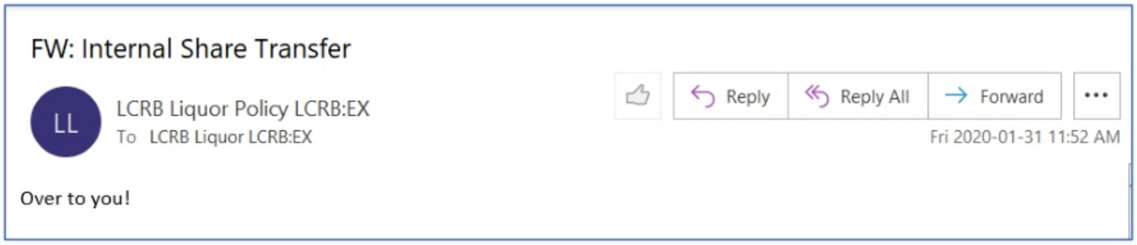


FW: Ubrew/Uvin Licence Renewal

LCRB Liquor Policy LCRB:EX
To LCRB Liquor LCRB:EX

Mon 2020-02-03 7:44 AM

Over to you!



FW: Internal Share Transfer

LCRB Liquor Policy LCRB:EX
To LCRB Liquor LCRB:EX

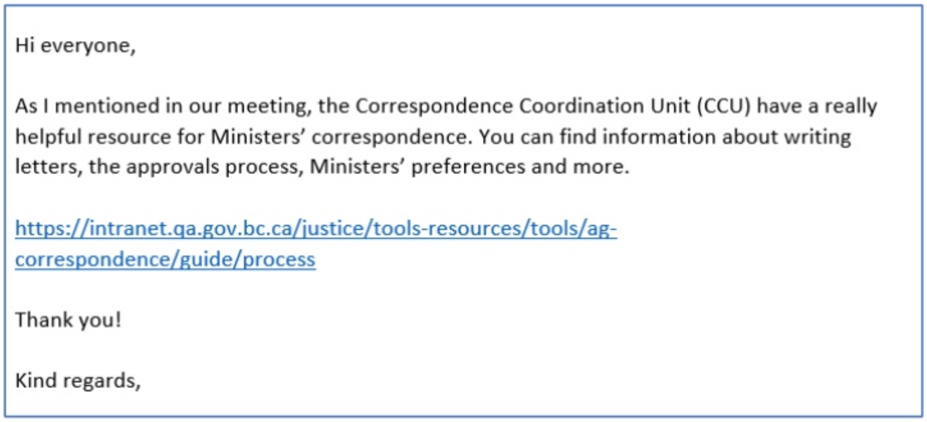
Fri 2020-01-31 11:52 AM

Over to you!

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

The emails below record day-to-day work relating to government business, but they don't document any significant actions or decisions and can be destroyed as ROTT.



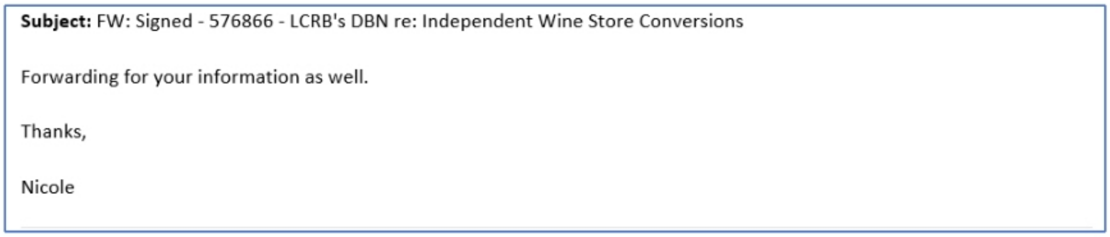
Hi everyone,

As I mentioned in our meeting, the Correspondence Coordination Unit (CCU) have a really helpful resource for Ministers' correspondence. You can find information about writing letters, the approvals process, Ministers' preferences and more.

https://intranet.qa.gov.bc.ca/justice/tools-resources/tools/ag-correspondence/guide/process

Thank you!

Kind regards,

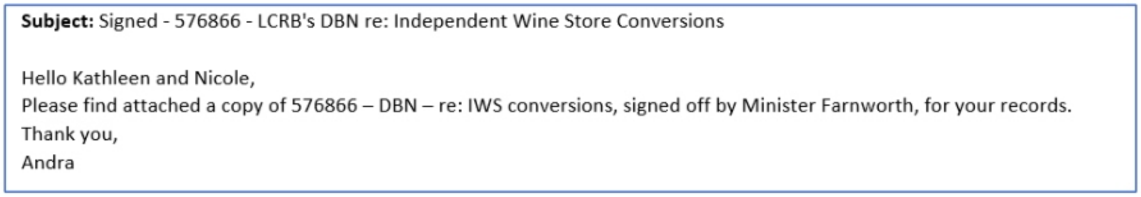


Subject: FW: Signed - 576866 - LCRB's DBN re: Independent Wine Store Conversions

Forwarding for your information as well.

Thanks,

Nicole



Subject: Signed - 576866 - LCRB's DBN re: Independent Wine Store Conversions

Hello Kathleen and Nicole,
Please find attached a copy of 576866 – DBN – re: IWS conversions, signed off by Minister Farnworth, for your records.
Thank you,
Andra

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

ROTT is detrimental in five important ways. First, it creates excessive storage, infrastructure and maintenance costs. Second, it impairs employees' ability to demonstrate compliance with regulatory guidelines or respond to FOI requests. Third, it impairs employees' ability to quickly access the right information and make data-driven decisions in an agile manner. Fourth, ROTT is often unmanaged and consequently, is vulnerable to data breaches. And fifth, information that is retained beyond its legal retention period poses a liability risk because it can be used against the organization in legal actions or financial audits.

Redundant

Is data that has duplicates stored across multiple locations, perhaps on a different system entirely, perhaps on the system. Intranet systems often contain a large amount of redundant data.

Obsolete

As the name suggests, is information that is no longer accurate or no longer in use. It might be outdated information that has been replaced. It is important to note that not all obsolete files can be arbitrarily deleted. It is only rendered obsolete, if it doesn't fall into the ARCS or ORCS classification. Many government records may appear obsolete but still have a retention schedule.

Transitory

Are government records that have short-term use only and do not need to be filed. They are produced or received in the course of routine actions, in the preparation of other records which replace them, or for convenient reference.

Trivial

Is information that isn't necessary to store. It is data that is providing no value to the organization and could be easily removed without any change to the business.

Management Services – Records

Project: *Electronic File Cleanup and Reorganization*

Destruction Tracker 2023 (FILES)

GM Shared		TOTALS
		0
ROTT	4411	4411
Formal	4025	4025
		0
		0
		0
Totals	**8436**	**8436**

Destruction Tracker 2023 (GB)

GM Shared		TOTALS
		0
		0
ROTT	0.36	0.36
Formal	0.425	0.425
		0
		0
Totals	**1**	**1**

Destruction Tracker 2023 (FILES)

LCL_Staffinfo		TOTALS
		0
ROTT	871	871
Formal	2063	2063
		0
		0
		0
Totals	**2934**	**2934**

Destruction Tracker 2023 (GB)

LCL_Staffinfo		TOTALS
		0
		0
ROTT	0.232	0.232
Formal	5.09	5.09
		0
		0
Totals	**5**	**5**

s. 14

s. 14

s. 14

s. 14

s. 14

s. 14

s. 14

Destruction Tracker 2022-2023 (FILES)		
C&E -Admin		TOTALS
		0
		0
ROTT	49	0
Formal	2668	0
		0
		0
Totals	2717	0

Destruction Tracker 2022-2023 (GB)		
C&E - Admin		TOTALS
		0
		0
ROTT	1.53	1.53
Formal	0.331	0
		0
		0
Totals	1.861	2

PSSG PSD FOI PSSG:EX

From: PSSG PSD FOI PSSG:EX
Sent: Monday, November 29, 2021 3:26 PM
To: Castillo, Billy R PSSG:EX; Lewis, Glen PSSG:EX; Pilling, David PSSG:EX; Sims, Brian A PSSG:EX; Lymburner, Ward C PSSG:EX; Lipp, Jamie M PSSG:EX; Gunnarson, Jess PSSG:EX; Brown, Matthew G PSSG:EX; Rideout, Wayne PSSG:EX; Winegarden, Cole PSSG:EX
Cc: Tupper, Linsey PSSG:EX; Levesque, Starr PSSG:EX; Grove, Juliet PSSG:EX; Khelawan, Sharon PSSG:EX; Singh, Roohi PSSG:EX; Sangha, Jivan PSSG:EX; Lamoureux, Tanya PSSG:EX
Subject: FYI - FOIPPA Royal Assent and impacts to PSB

Hi Exec team,

There have been some changes to the FOIPPA legislation that the executive team should be informed of. I don't think the changes will impact PSB much, it will mostly be on the processing side at IAO, but it's good to be informed. The changes to legislation are captured here:

Bill 22 – 2021: Freedom of Information and Protection of Privacy Amendment Act, 2021 (leg.bc.ca)

Here is my overview for PSB:

- First – there is a new $10 application fee for all general requests going forward as of November 29, 2021. This will be processed by the IAO intake team before the request reaches us. **May reduce number of general requests – nominal effect to PSB**

- Second – the bill was reviewed with an Indigenous lens. Much of the language has been updated to reflect this.

    - Section 16 – Intergovernmental relations or negotiations.
        - There are new protections to Indigenous Governing Entities (previously "aboriginal governments") that allow them to withhold records that have been in existence longer than 15 years). **Little to no impact on PSB** – law enforcement information was already exempt from the 15 years AND our FOIs tend to ask for current records.

    - Section 18 – Conservation of heritage sites
        - NEW MANDATORY exception. This exception is now expanded to include "Disclosure harmful to interests of an Indigenous people." 18.1 (1) The head of a public body must refuse to disclose information if the disclosure could reasonably be expected to harm the rights of an Indigenous people to maintain, control, protect or develop any of the following with respect to the Indigenous people: (a) cultural heritage; (b) traditional knowledge; (c) traditional cultural expressions; (d) manifestations of sciences, technologies or cultures. (2) Subsection (1) does not apply if the Indigenous people has consented in writing to the disclosure. **Little to no impact on PSB –** this is a conservation exemption that PSB has never applied to my knowledge. NOTE – there is an update to section 23 – notifying the third party, applying the scheme for third party notice to the new disclosure exception. This is on IAO to provide written notice (but we can always identify for them).
- Third - Section 43 - The power to authorize a public body to disregard requests was expanded.
    - The criteria that the Commissioner can use to authorize a public body to disregard a request has expanded to include when: the request is for a record that has been disclosed to the applicant or that is accessible by the applicant from another source, or; responding to the request would unreasonably

interfere with the operations of the public body because the request; is excessively broad or is repetitious or systematic. **May impact PSB –** IAO is not yet sure of the process, but if we suspect a request to be vexatious and intentionally disruptive, we now have the right to question the call for records.

** If you believe any OPEN FOI cases are affected by these updates, please let me know ASAP.

Please let me know if you have any questions. If I can't answer, I can facilitate a conversation with IAO.
Please forward to your directors, and note that Billy will inform BMC.

Thanks,
Carolyn Wilcher
Program Analyst
Policing and Security Branch
Public Safety and Solicitor General
778-974-4818

A safe, secure, just, and resilient British Columbia

I acknowledge and respect the Lekwungen-speaking Peoples on whose traditional territories I live, work, and enjoy, and the Songhees, Esquimalt and WSANEC peoples whose historical relationships with the land continue to this day.

Defensible Internal Business Process for Records Destruction

Policing and Security Branch

Purpose

The purpose for this business Process is to establish a defensible, documented, and consistent process for Policing and Security Branch (PSB) to legally destroy eligible records. This document covers the process for physical and electronic records destruction and does not include the destruction of data or decommissioning systems.

Background

Citizens' Services' Government Records Service (GRS) has centrally held the authority to approve records destruction applications. The program areas would prepare an application, submit it for internal approval, then GRS would have final approval authority. In January 2023, GRS is delegating that authority to the ministries. Within the Justice Sector, branches are responsible for the entirety of their destruction process (creating, enacting, and approving). The process detailed here follows GRS's guidelines and adheres to the *Information Management Act.*

Roles and Responsibilities

It is recommended, but not required, that the following 3 roles be held by separate people for any given destruction.

Preparer(s)

Anyone can create and prepare a file list. They are responsible for identifying the records that need to be destroyed, creating the file list, ensuring the dates and retention schedules are correct and eventually destroying or deleting the records.

Reviewer(s)

PSB's reviewers will be Analysts charged with information management the reviewer has 2 duties:

1) Logging: Reviewer will generate the IDA number, ensuring each application has a unique number and the year in which it was destroyed.
2) Reviewing: They will be responsible for reviewing the file list created as outlined below

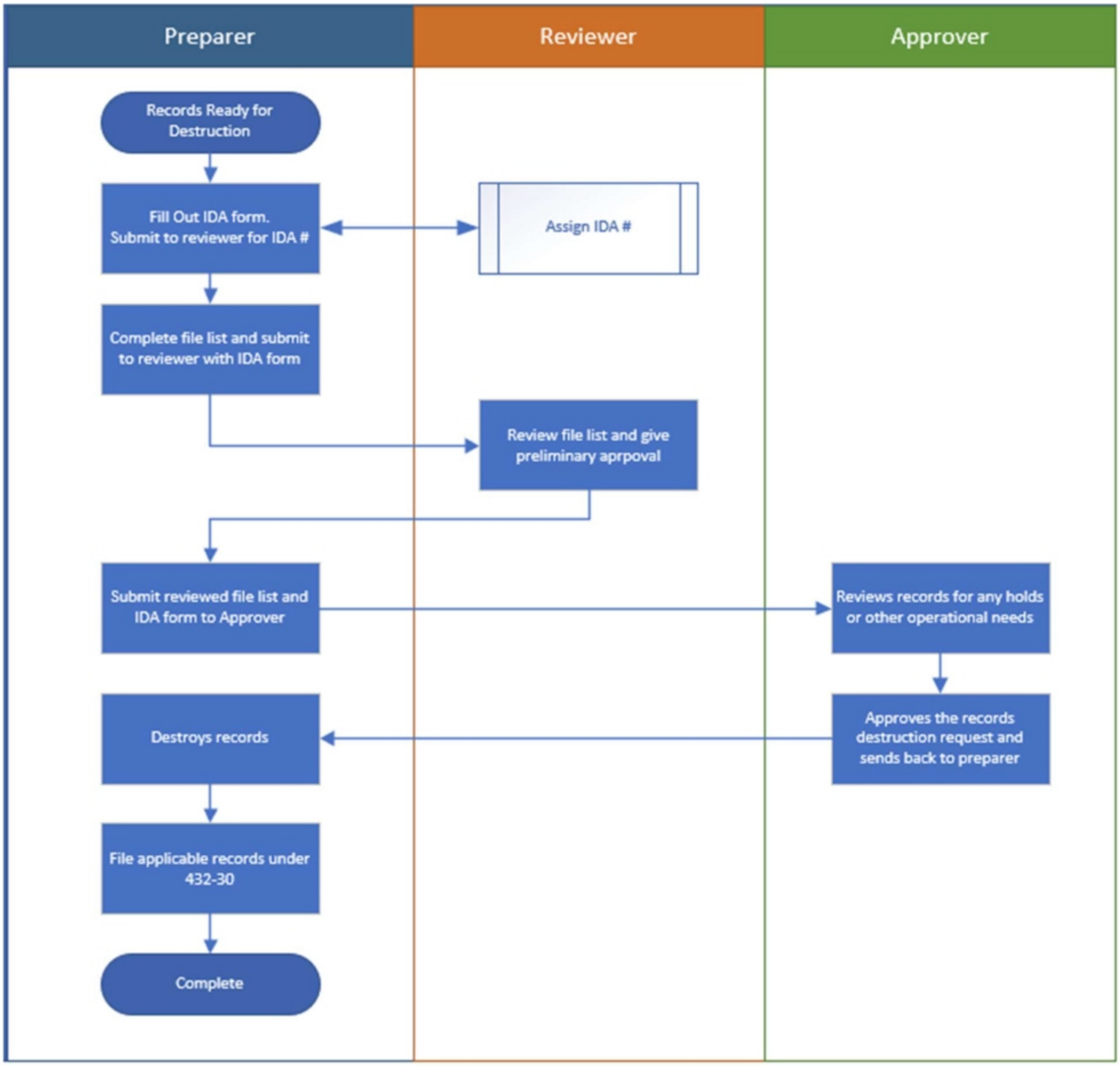
Approver(s):

Executive Directors whose areas either created the records, are current custodian of the records, or are known to have a business interest in the records. The approver(s) are responsible for ensuring the records being destroyed are not part of any FOI, litigation, audit, or required for any operational need.

Process

The following steps are now internal to PSB and are considered adequate and defensible for legal destruction of records. This process can be used for the onsite destruction of physical records (e.g., paper files, audiovisual records, photos, computer tapes, diskettes, etc.) and destruction of digital information (e.g., LAN records, EDRMS e-records, records residing in systems, and other digital storage locations.)

Flow Chart


Preparer
Reviewer
Approver
Records Ready for Destruction
Fill Out IDA form. Submit to reviewer for IDA #
Assign IDA #
Complete file list and submit to reviewer with IDA form
Review file list and give preliminary arpproval
Submit reviewed file list and IDA form to Approver
Reviews records for any holds or other operational needs
Approves the records destruction request and sends back to preparer
Destroys records
File applicable records under 432-30
Complete

Detailed Steps

Preparer

1. Review the records to ensure the retention period has been reached.
2. Complete Information Destruction Application (IDA) Form (Appendix A) and submit to reviewer.
   a. The **reviewer** will assign the IDA # with the below naming convention.
      i. **DE**YY-###-**PSSG-PSB**
      ii. YY = calendar year
      iii. ### = sequential number, starting with 001 each year
3. Complete a file list (Appendix B) which must include the below:
   a. Schedule Number
   b. Box Number (if applicable)
   c. File Title/Description

   d. Classification – Primary and Secondary
   e. Office of the Primary Responsibility (OPR) Y/N
   f. Start Date
   g. Superseded or Obsolete (SO) Date (if applicable)
   h. End Date based on SO date or retention schedule
   i. Final Disposition Date

4. Submit completed file list with IDA to **reviewer**

Reviewer

5. Confirm that final disposition dates have been calculated correctly,
6. Ensure that all classifications included within the destruction are approved and can be destroyed (i.e., no records classified under a draft schedule. Schedules can be approved but have classifications within the schedule that are draft.
7. Review file titles, classifications, retention schedules, and look for red flags and anomalies.
8. Request any additional information or clarification in writing, that will be filed with the destruction case.
9. Preliminarily approve the file list
10. Return the file list and IDA to **preparer** to submit to **approver**

Approver

11. Confirm that no holds apply to any of the records (i.e., for FOI, litigation, audit, etc.)
12. Confirm there is no further operational need for the records.
13. Approves the destruction through digital signature on the IDA form or email approval saved as PDF and attached to IDA form.
14. Approved IDA form and file list returned to **preparer**

Preparer

15. Once approved, the records are to be destroys through shredding services or file deletion as soon as possible.
16. Approved IDA form, final file list, and any other applicable records are to be filed under 432-30 Destruction Case Files. CY+30Y Nil DE
17. Ensure any applicable tracking systems or database programs reflect the status of the destroyed files.
18. The preparer ensures all approved logs, file lists, supporting documentation, and approvals will be filed under 432-30 Destruction case files – internal for CY+30y nil DE in the official records keeping system.
19. After records have been destroyed, ensure all applicable tracking systems are updated to reflect the “destroyed” status of the records**.**

Redundant Source Records Destruction Process (Digitization of Records)

Policing and Security Branch

Purpose

The purpose for this business Process is to establish a defensible, documented, and consistent process for Policing and Security Branch (PSB) to legally destroy redundant source records after the records have been digitized.

Background

Citizens' Services' Government Records Service (GRS) has centrally held the authority to approve records destruction applications. The program areas would prepare an application, submit it for internal approval, then GRS would have final approval authority. In January 2023, GRS is delegating that authority to the ministries. Within the Justice Sector, branches are responsible for the entirety of their destruction process (creating, enacting, and approving). The process detailed here follows GRS's guidelines and adheres to the *Information Management Act.*

Roles and Responsibilities

It is recommended, but not required, that the following 3 roles be held by separate people for any given destruction.

Preparer(s)

The preparer must review the RSR guide (Appendix A) to ensure the records are eligible for redundant source record destruction. They will be the one(s) to fill out the Digitization Process Worksheet and be the one digitizing the records. Once the records are confirmed to be full in their digitized state, the preparer will also destroy the records.

Reviewer(s)

PSB's reviewers will be Analysts charged with information management the reviewer has 2 duties:

1) Logging: Reviewer will generate the IDA number, ensuring each application has a unique number and the year in which it was destroyed.
2) Reviewing: They will be responsible for reviewing the Digitization Process Worksheet before the approver to ensure the appropriate process is in place.

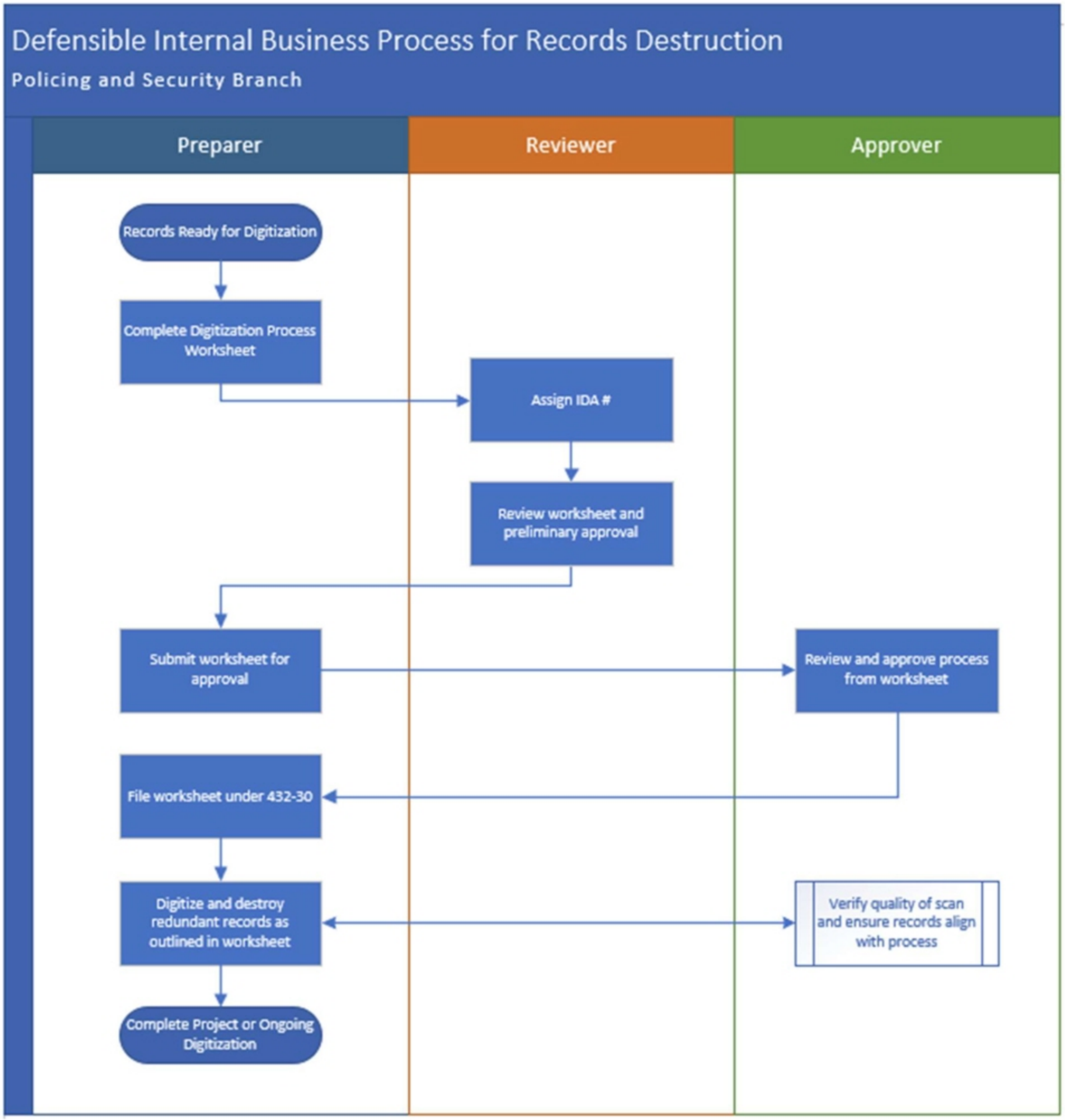
Approver(s):

Executive Directors whose areas either created the records, are current custodian of the records, or are known to have a business interest in the records. The approver(s) are responsible for ensuring the digitization process is being followed as outlined in the process worksheet.

Process

The following steps are now internal to PSB and are considered adequate and defensible for legal destruction of redundant source records after the records have been digitized. The process can be used for a one-off project to digitize older records, or can be used as an ongoing basis for records that have to be continuously digitized.

Flow Chart


Defensible Internal Business Process for Records Destruction
Policing and Security Branch
Preparer
Reviewer
Approver
Records Ready for Digitization
Complete Digitization Process Worksheet
Assign IDA #
Review worksheet and preliminary approval
Submit worksheet for approval
Review and approve process from worksheet
File worksheet under 432-30
Digitize and destroy redundant records as outlined in worksheet
Verify quality of scan and ensure records align with process
Complete Project or Ongoing Digitization

Detailed Steps

Preparer

1. Review the records to ensure the RSR can be used.
2. Complete Digitization Process Worksheet (Appendix B) and submit to reviewer.

Reviewer

3. Assign the IDA# with the below naming convention
   a. **DE**YY-###-**PSSG-PSB**
   b. YY = calendar year
   c. ### = sequential number, starting with 001 each year

4. Ensure the process outline aligns with the information management act and thorough processes are in place for preparation and digitizing of the records.
5. Confirm with the preparer where the records will be stored and ensure proper labelling and classification.
6. Confirm the SR and FR records do not have unique physical elements, or are not maps, designs, drawings, or artwork.
7. Preliminarily approve the Digitization Process Worksheet
8. Return the file list and IDA to **preparer** to submit to **approver**

Approver

9. Confirm there the processes from the worksheet align with business practices.
10. Work with the preparer on plan to verify the scan quality throughout the process.
11. Approves the Digitization Process Worksheet through email as PDF attached.
12. Approved worksheet is sent back to the **preparer**

Preparer

13. The approved Digitization Process Worksheet needs to be labelled and filed under 432-30
14. Records can now be digitized and redundant source records destroyed as outlined in the worksheet

s. 14

s. 14

s. 14

s. 14

s. 14

s. 14

From: Skogstad, Holly AG:EX
To: Butler, Sylvia GPEB:EX; Truong, My Anh GPEB:EX; Lewis, Jamie GPEB:EX
Subject: RE: Centralize FOI process
Date: July 29, 2022 11:13:07 AM

Good Morning,

Apologies on the delay in getting back to you. The process looks good and the additions with the centralized FOI coordinator are correct.

I am happy to have My Ahn present the changes to the FOI Process at the Executive meeting but will note I am also able to attend if I was wanted/needed for any questions or concerns (I feel everything is outlined clearly in the process and I should not be needed but I am happy to make myself available)

Thank you all for your cooperation with these process changes and for making my job easier.

Have a great long weekend.

Holly Skogstad

Central FOI Coordinator

(778) 698-3889| holly.skogstad@gov.bc.ca

From: Butler, Sylvia GPEB:EX <Sylvia.Butler@gov.bc.ca>
Sent: Tuesday, July 26, 2022 3:23 PM
To: Skogstad, Holly AG:EX <Holly.Skogstad@gov.bc.ca>; Truong, My Anh GPEB:EX <MyAnh.Truong@gov.bc.ca>; Lewis, Jamie GPEB:EX <Jamie.L.Lewis@gov.bc.ca>
Subject: Centralize FOI process

Hi Holly, please find attached the revised Visio flowchart with new process as I understand it. Can you review the attached two documents and let me know if I missed anything.

Once you have reviewed I can review with My Anh and Jamie Lewis (who I am including in this email) and then they can review with Executive and ADM to share the changes in FOI process for the Ministry.

<< File: GPEB _ FOI _ PROCESS _FLOWCHART _ Rev _ 202200726.vsdx >>

<< File: FOI-ProcessCheatSheet-Final-20220726.docx >>

My Anh and Jamie, Holly has offered to attend Executive meeting to go over new process if you would like her to do that for you.

Again, if you require changed to the documents, please let me know. Once signed off by everyone I can update my detailed procedures manual. Thanks.

Yours truly,

Sylvia Butler

FOI and Records Management Officer - Team Lead| Gaming Enforcement and Policy Branch |Ministry of Public Safety and Solicitor General, *3rd Floor, 910 Government Street*
Victoria, BC   V8W 9N1 |Telephone: 778-698-5544

For any FOI inquiries please email GPEB's FOI email box GPEB.FOIManagement@gov.bc.ca.
For any EDRMS access authorizations and or records questions, please email GPEB's Record Management mailbox GPEB_RecordsManagement@gov.bc.ca.

*** CONFIDENTIALITY NOTICE***
This communication (both the message and any attachments) is intended for use by the person or persons to whom it is addressed and must not be shared or disseminated unless authorized by law or with the express authority of the sender. This communication may contain privileged or confidential information. If you have received this message in error or are not the named recipient, please immediately notify the sender and delete the message from your mailbox and trash without copying or disclosing it.***

Proposed GPEB FOI process

- FOI request is received at IAO Flex Team
- IAO Flex team sends the request to the Central FOI coordinator for distribution. Once it is decided that the request should be directed to GPEB, the central FOI Coordinator will forward the CFR to GPEB for circulation.
    - Native files can be sent directly to the Central FOI Coordinator for de-duplication. As discussed, the FileShare will continue to be used for uploading.
    - NRRs, Fee Estimates and consults will be directed through the Central FOI Coordinator for streamlining.
- Central FOI Coordinator combines all records for the request on the FileShare for De-duplication at IAO
- Once the file has been de-duplicated, IAO Flex team will advise the Central FOI Coordinator that it is ready for Harms assessment.
- Central FOI coordinator will send it to GPEB for harms review.
    - The Branch will review the file and note possible harms in the records.
    - Once review is complete, the file can be sent back to the Central FOI Coordinator

- Once the records have been reviewed, the central FOI coordinator will advise the IAO Justice team when records are ready.
- IAO Justice team will apply the redlines, request consults and ensure consistent severing if it is a multi-ministry request.
- IAO Justice team sends the central FOI coordinator the sign off package for final review and distribution.
- NRR's from GPEB can be preapproved in eApprovals ADM McLeod or a designated executive to review and approve.
- Central Coordinator will forward the package to GPEB. Sign off package will be uploaded to eApprovals for circulation.
    - The Branch will receive final sign off package in eApprovals for review and approval.
    - Any additions to the redline can be requested in eApprovals and sent to the Central FOI Coordinator. The Central FOI Coordinator will work with IAO to have the additions applied and uploaded the revised redline for review.
    - Note: there may be records from more that one area. When there is more than one area in a package, the pages will be identified or possibly 2 redlines attached and named accordingly (depending upon how IAO processes it)
    - Once the package is approved by ADM McLeod or Designated Executive, the package can be sent to the Central FOI coordinator.
    - E-signatures no longer need to be applied to the CFR or Sign off documents. Going forward we will use the eApproval history.
- **If package requires DSG sign off, the central FOI coordinator will send it to the DSG in eApprovals.**
- Central FOI coordinator will send the completed approved sign off package to IAO for closing and distribution to the applicant.

From:	AG PSSG FOI Coordinator AG:EX
To:	GPEB FOI Management GPEB:EX
Cc:	AG PSSG FOI Coordinator AG:EX
Subject:	Proposed Central FOI Coordinator
Date:	July 7, 2022 10:51:42 AM
Attachments:	Proposed GPEB FOI Process.docx

Good Morning,

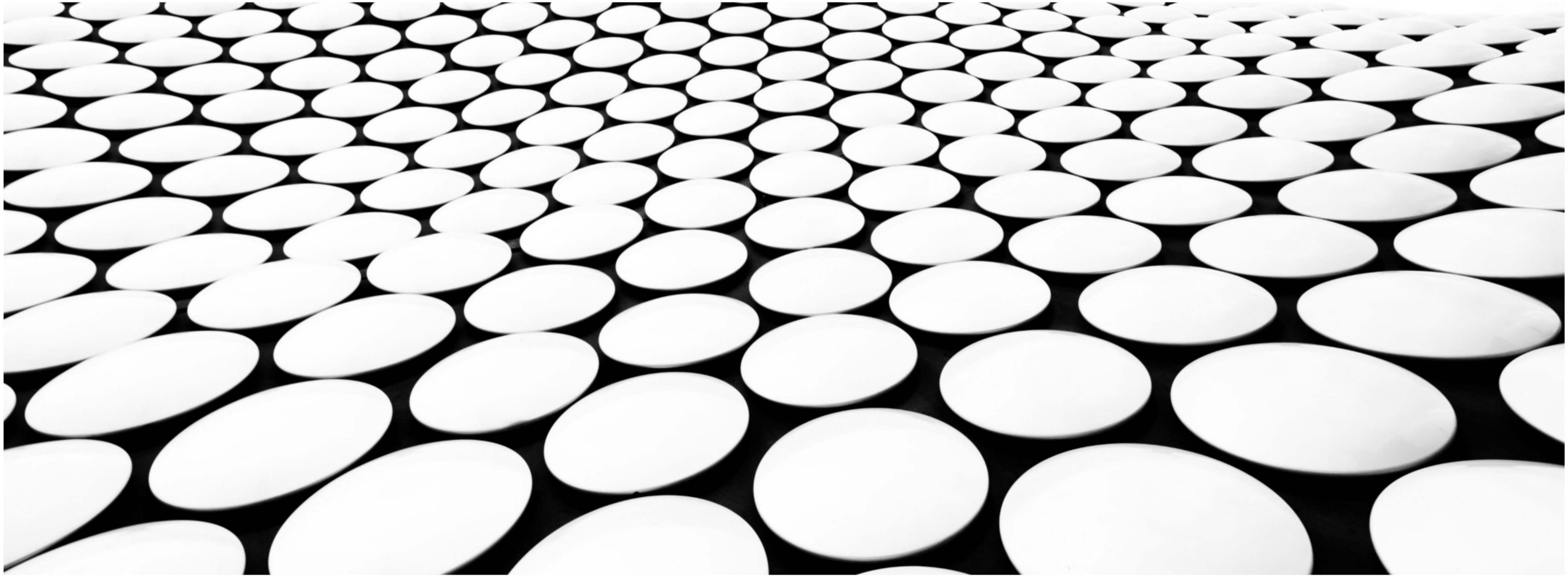
As Discussed yesterday, here are a centralized proposed procedures. Please review and let me know if you have any additions, changes or questions.
I appreciate you taking the time yesterday.

Thank you

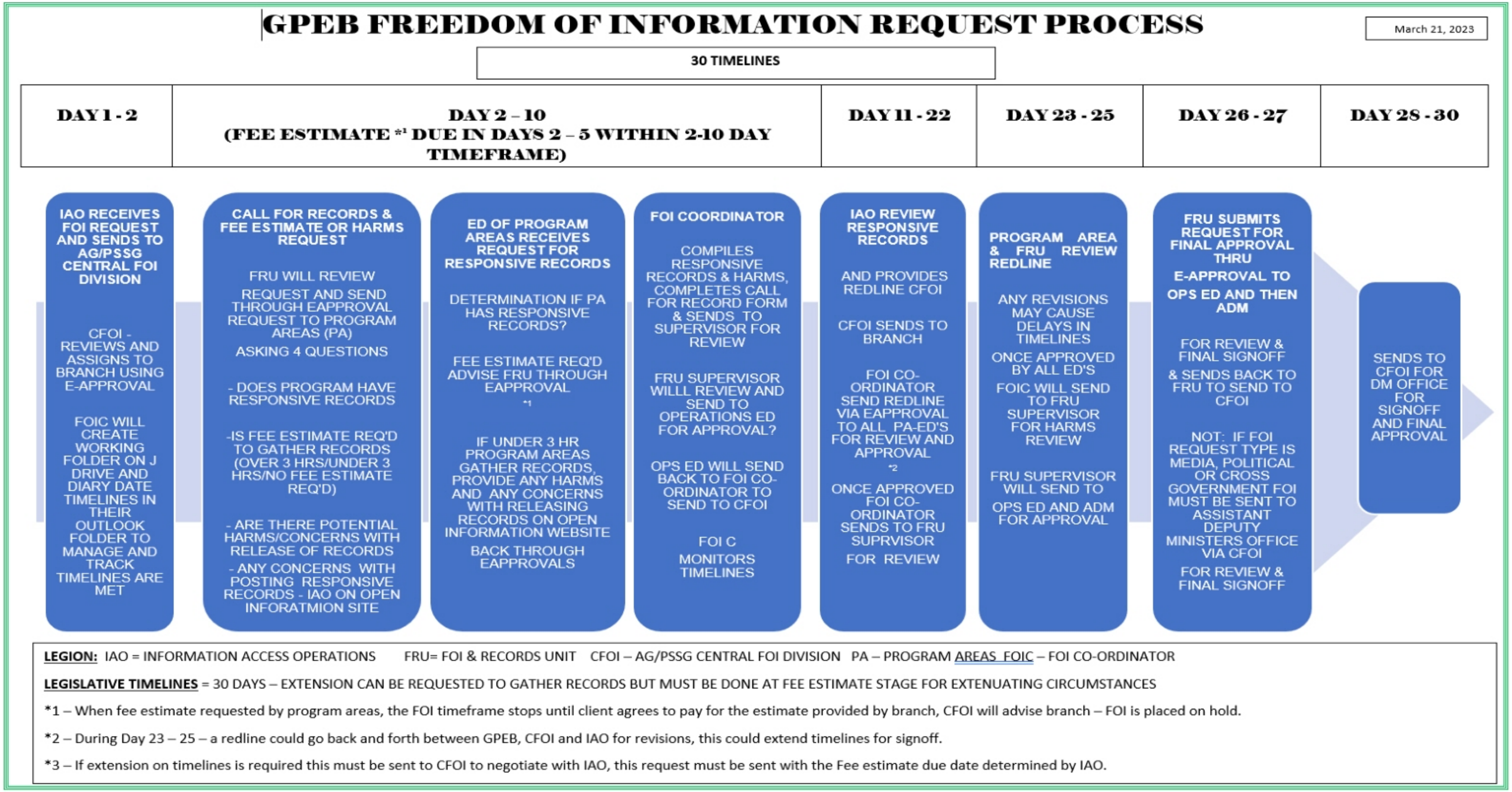
Holly Skogstad
Central FOI Coordinator
Information Systems Branch
Ministry of Attorney General
(778) 698-3889 | agpssg.foicoordinator@gov.bc.ca

GPEB FOI PROCESS

20230413



CURRENT FOI PROCESS



GPEB FREEDOM OF INFORMATION REQUEST PROCESS

March 21, 2023

30 TIMELINES

DAY 1 - 2	DAY 2 – 10 (FEE ESTIMATE *1 DUE IN DAYS 2 – 5 WITHIN 2-10 DAY TIMEFRAME)	DAY 11 - 22	DAY 23 - 25	DAY 26 - 27	DAY 28 - 30

IAO RECEIVES FOI REQUEST AND SENDS TO AG/PSSG CENTRAL FOI DIVISION

CFOI - REVIEWS AND ASSIGNS TO BRANCH USING E-APPROVAL

FOIC WILL CREATE WORKING FOLDER ON J DRIVE AND DIARY DATE TIMELINES IN THEIR OUTLOOK FOLDER TO MANAGE AND TRACK TIMELINES ARE MET

CALL FOR RECORDS & FEE ESTIMATE OR HARMS REQUEST

FRU WILL REVIEW

REQUEST AND SEND THROUGH EAPPROVAL REQUEST TO PROGRAM AREAS (PA)

ASKING 4 QUESTIONS

- DOES PROGRAM HAVE RESPONSIVE RECORDS

-IS FEE ESTIMATE REQ'D TO GATHER RECORDS (OVER 3 HRS/UNDER 3 HRS/NO FEE ESTIMATE REQ'D)

- ARE THERE POTENTIAL HARMS/CONCERNS WITH RELEASE OF RECORDS

- ANY CONCERNS WITH POSTING RESPONSIVE RECORDS - IAO ON OPEN INFORATMION SITE

ED OF PROGRAM AREAS RECEIVES REQUEST FOR RESPONSIVE RECORDS

DETERMINATION IF PA HAS RESPONSIVE RECORDS?

FEE ESTIMATE REQ'D ADVISE FRU THROUGH EAPPROVAL
*1

IF UNDER 3 HR PROGRAM AREAS GATHER RECORDS, PROVIDE ANY HARMS AND ANY CONCERNS WITH RELEASING RECORDS ON OPEN INFORMATION WEBSITE

BACK THROUGH EAPPROVALS

FOI COORDINATOR

COMPILES RESPONSIVE RECORDS & HARMS, COMPLETES CALL FOR RECORD FORM & SENDS TO SUPERVISOR FOR REVIEW

FRU SUPERVISOR WILLL REVIEW AND SEND TO OPERATIONS ED FOR APPROVAL?

OPS ED WILL SEND BACK TO FOI CO-ORDINATOR TO SEND TO CFOI

FOI C

MONITORS TIMELINES

IAO REVIEW RESPONSIVE RECORDS

AND PROVIDES REDLINE CFOI

CFOI SENDS TO BRANCH

FOI CO-ORDINATOR SEND REDLINE VIA EAPPROVAL TO ALL PA-ED'S FOR REVIEW AND APPROVAL
*2

ONCE APPROVED FOI CO-ORDINATOR SENDS TO FRU SUPRVISOR

FOR REVIEW

PROGRAM AREA & FRU REVIEW REDLINE

ANY REVISIONS MAY CAUSE DELAYS IN TIMELINES

ONCE APPROVED BY ALL ED'S

FOIC WILL SEND TO FRU SUPERVISOR FOR HARMS REVIEW

FRU SUPERVISOR WILL SEND TO

OPS ED AND ADM FOR APPROVAL

FRU SUBMITS REQUEST FOR FINAL APPROVAL THRU

E-APPROVAL TO

OPS ED AND THEN ADM

FOR REVIEW & FINAL SIGNOFF

& SENDS BACK TO FRU TO SEND TO CFOI

NOT: IF FOI REQUEST TYPE IS MEDIA, POLITICAL OR CROSS GOVERNMENT FOI MUST BE SENT TO ASSISTANT DEPUTY MINISTERS OFFICE VIA CFOI

FOR REVIEW & FINAL SIGNOFF

SENDS TO CFOI FOR DM OFFICE FOR SIGNOFF AND FINAL APPROVAL

LEGION: IAO = INFORMATION ACCESS OPERATIONS   FRU= FOI & RECORDS UNIT   CFOI – AG/PSSG CENTRAL FOI DIVISION   PA – PROGRAM AREAS FOIC – FOI CO-ORDINATOR

LEGISLATIVE TIMELINES = 30 DAYS – EXTENSION CAN BE REQUESTED TO GATHER RECORDS BUT MUST BE DONE AT FEE ESTIMATE STAGE FOR EXTENUATING CIRCUMSTANCES

*1 – When fee estimate requested by program areas, the FOI timeframe stops until client agrees to pay for the estimate provided by branch, CFOI will advise branch – FOI is placed on hold.

*2 – During Day 23 – 25 – a redline could go back and forth between GPEB, CFOI and IAO for revisions, this could extend timelines for signoff.

*3 – If extension on timelines is required this must be sent to CFOI to negotiate with IAO, this request must be sent with the Fee estimate due date determined by IAO.

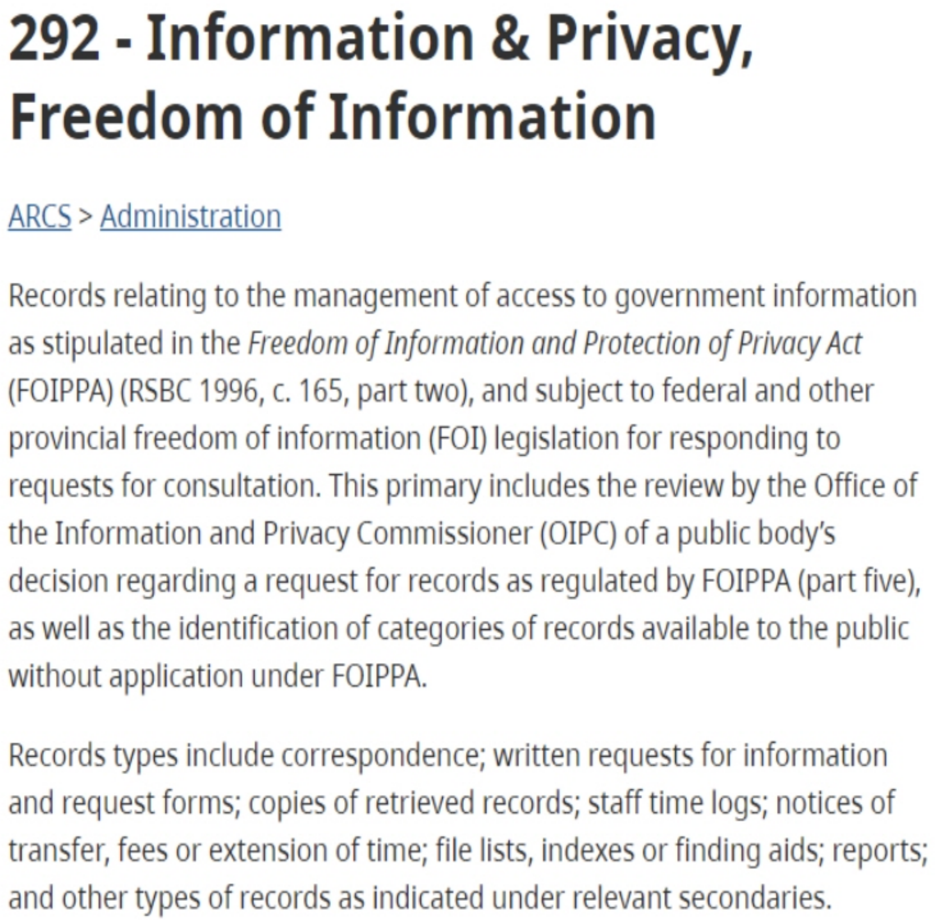
FOI STATISTICS

- 2013 & 2014 – 69 folders create – none closed – created as Non-OPR records
- 2015 – 2 folders – not closed – created as Non-OPR records
- 2016 – 1 folder created not closed – created as OPR
- 2017 – 47 folders created – none closed – entered as OPR
- 2018 – 74 folders created – none closed – entered as OPR – 11 empty folders – no contents
- 2019 – 42 folders created – none closed – entered as OPR (16 to be added to EDRMS)
- 2020 – 4 entered in EDRMS – 32 to be entered
- 2021 - 21 to be entered into EDRMS
- 2022 – 24 to be entered into EDRMS
- 2023 – 4 to be entered into EDRMS

Issue: 2012 IAO took on the responsibility of OPR for FOI requests.

Question: Does anyone know why we changed from Non-OPR to OPR in 2016? Was this because of the reviews MNP/Peter German/Cullen Commission Inquiry?

CLASSIFICATIONS RELATED TO FOI'S



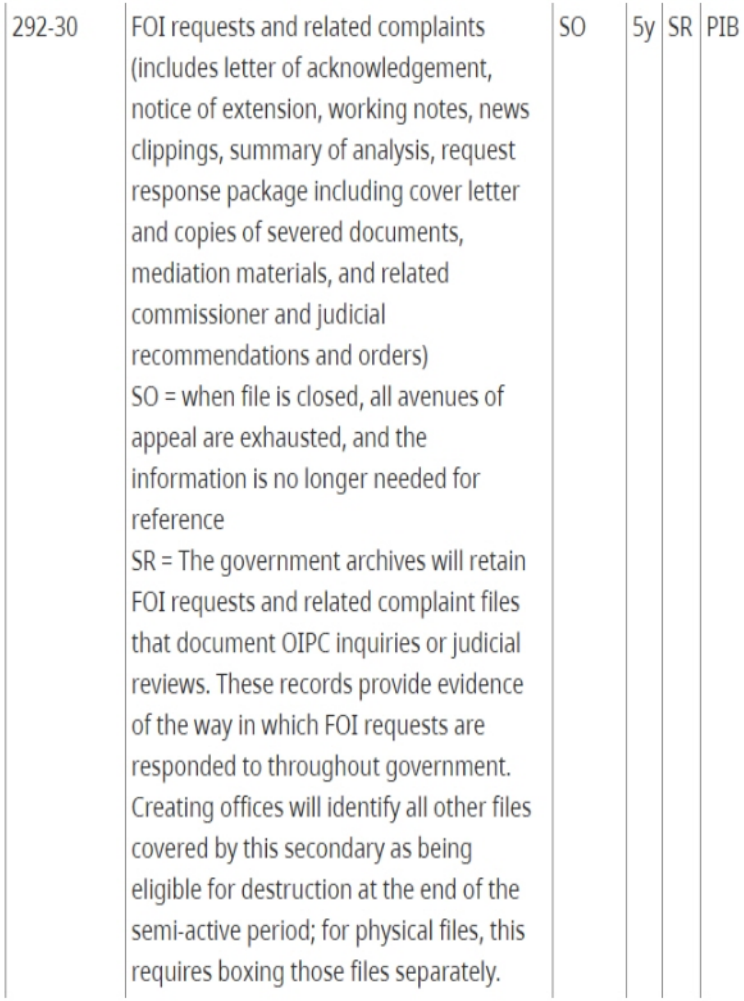
292 - Information & Privacy, Freedom of Information

ARCS > Administration

Records relating to the management of access to government information as stipulated in the *Freedom of Information and Protection of Privacy Act* (FOIPPA) (RSBC 1996, c. 165, part two), and subject to federal and other provincial freedom of information (FOI) legislation for responding to requests for consultation. This primary includes the review by the Office of the Information and Privacy Commissioner (OIPC) of a public body's decision regarding a request for records as regulated by FOIPPA (part five), as well as the identification of categories of records available to the public without application under FOIPPA.

Records types include correspondence; written requests for information and request forms; copies of retrieved records; staff time logs; notices of transfer, fees or extension of time; file lists, indexes or finding aids; reports; and other types of records as indicated under relevant secondaries.

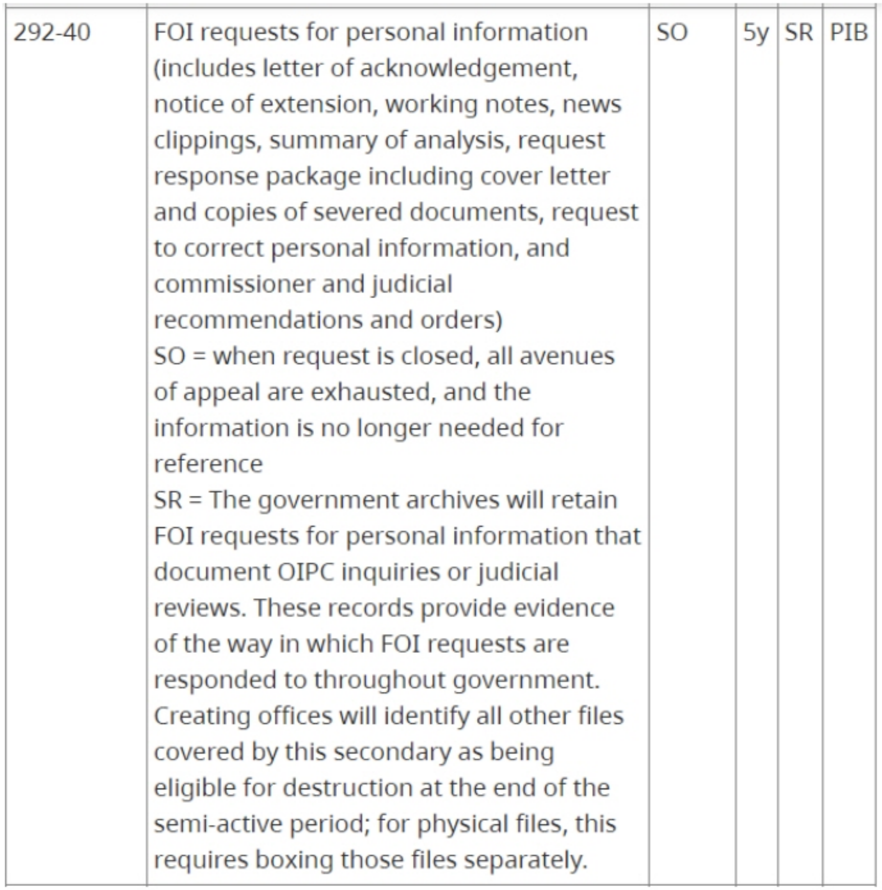
FOI General Requests:



292-30	FOI requests and related complaints (includes letter of acknowledgement, notice of extension, working notes, news clippings, summary of analysis, request response package including cover letter and copies of severed documents, mediation materials, and related commissioner and judicial recommendations and orders) SO = when file is closed, all avenues of appeal are exhausted, and the information is no longer needed for reference SR = The government archives will retain FOI requests and related complaint files that document OIPC inquiries or judicial reviews. These records provide evidence of the way in which FOI requests are responded to throughout government. Creating offices will identify all other files covered by this secondary as being eligible for destruction at the end of the semi-active period; for physical files, this requires boxing those files separately.	SO	5y	SR	PIB

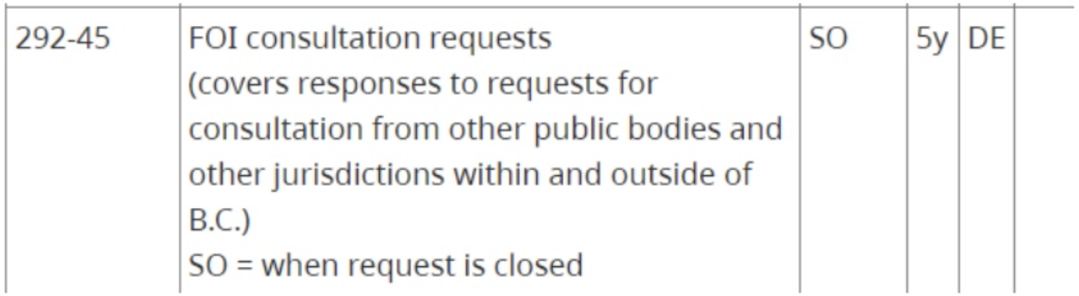
CLASSIFICATIONS RELATED TO FOI'S

FOI Personal Requests:

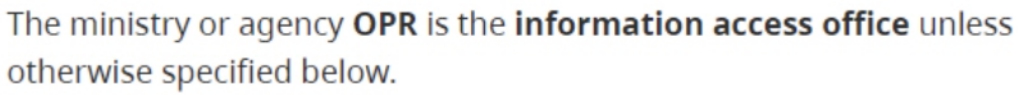


292-40	FOI requests for personal information (includes letter of acknowledgement, notice of extension, working notes, news clippings, summary of analysis, request response package including cover letter and copies of severed documents, request to correct personal information, and commissioner and judicial recommendations and orders) SO = when request is closed, all avenues of appeal are exhausted, and the information is no longer needed for reference SR = The government archives will retain FOI requests for personal information that document OIPC inquiries or judicial reviews. These records provide evidence of the way in which FOI requests are responded to throughout government. Creating offices will identify all other files covered by this secondary as being eligible for destruction at the end of the semi-active period; for physical files, this requires boxing those files separately.	SO	5y	SR	PIB

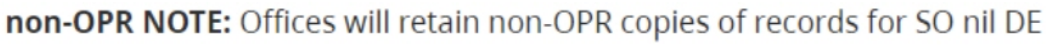
FOI Consultation requests



292-45	FOI consultation requests (covers responses to requests for consultation from other public bodies and other jurisdictions within and outside of B.C.) SO = when request is closed	SO	5y	DE



The ministry or agency **OPR** is the **information access office** unless otherwise specified below.



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

QUESTION:

- Is there a reason we file these records as Office of Primary Responsibility?

FOI AND RECORDS MANAGEMENT – FOI PROCESS-REVISED 20231003

The chart below reflects the timelines for an FOI request received at GPEB. Keep in mind IAO controls the timelines to meet the 30-day legislative requirements any extensions must be submitted to CFOI WHO WILL LIAISON WITH IAO.

TIME LINES	TASK	ROLE	DETAILS
DAY 1- 2	IAO SENDS FOI REQUEST TO CFOI	AG/PSSG – CFOI Division	CFOI – will review request, create Eapproval request and send to GPEB FOI Co-ordinator (FOIC). - Call for Records (CFR) - Harms Request on responsive records from another area
DAY 2 TO 5	GPEB Receives Request for Records / Harms requests from CFOI	FOIC	Will: - Create working folder in "J" LAN drive and save CFR form/Harms request in folder created. - Create Responsive Record (RR) folder in s. 17 RECORDS RESTRICTED FOLDER for PA's to place responsive records (if applicable) - Check historical FOI requests to see if previous/similar requests have been made. - Review request and forward Supervisor for review and action - Track due dates for FE/Responsive Due date and Legislative Date in Outlook calendar as a reminder to follow up with PA's if they have not met their timelines
	GPEB FOI and Records Mgmt. Officer	FOI-OTL	Will: - Received Eapproval for review and action from FOIC. - CFR – Programs to determine if responsive records exist. - Harms Request -Programs to identify any harms with responsive records provided by IAO. - Update Eapproval Route to identity who should be included in review. - Indicate 4 questions that must be answered by Program areas: - - Does Program area have responsive records? - - Is a Fee Estimate required? (Review Section 4 of the Call For Records form: - - over 3 hrs – Yes – how long and why - - under 3 hrs – No – start gathering PA's responsive records - - No responsive records - - Does PA require application to provide further clarification on scope? - **Note:** Program areas should also identify if other entities outside of GPEB may hold records and provide this information to the FOI Co-ordinator asap. - **Note:** Advise PA to COPY responsive records to following LAN drive location: (if applicable) s. 17 RECORDS RESTRICTED FOLDER. - ***Create folders for*** Call for Records - CFR, Responsive Records – RR & Redline Documents - RL

	Fee Action Review and OR Response Required By Due Date (S)	ED - all programs*	Will: Determine with their program areas if they have responsive records (RR) in any of the following locations: - LAN Drive (including H drive), GOS, CLIFF, Outlook (PST files Historical files), EDRMS, hard copy records / Records offsite/black/notebooks, storage keys or hard drives, CLIFF. - - Provide their responses to Fee Estimate if responsive records will take more than 3 hours to retrieve (see guidelines on Call for Records form (CFR): - Yes – RR – under 3 hours – Start gathering records. - No RR – note in Eapproval and move to next person in Eapproval route. - Does Program Area require further scope clarification? Note in Eapproval. - Are we aware of any third party that may have records? - Do program areas have any concerns with redline/severed documents being placed on Open Information Website? - **Note:** Responsive Records should be placed in following restricted drive: s. 17 RECORDS RESTRICTED FOLDER. – All ED's, ADMO and FRU have access to this folder. (Only if volume is too large for eapproval or the information is highly confidential). Team lead will gather records and change to pdf for Central FOI and IAO. .
DAY 2 TO 12	Check to ensure all programs have responded by due date for fee estimate or responsive records.	FOIC	ED's Will: - return RR to FOI Co-ordinator by due date to the designated shared drive if large responsive records or highly confidential: Under the corresponding FOIC will move records to LAN drive folder under the J drive FOI Pending folder with corresponding FOI request sub folder - Request Folder number i.e., MAG-YYYY-#####. - s. 17 RECORDS RESTRICTED FOLDER. - Complete Call for Records form (Section 3, 4, 5 and 7) with responses from program areas and send to FOIOTL - Supervisor for review and action.
DAY 2 TO 12	Results of review for RR sent to FOI TL	FOIOTL	Will: **If fee estimate required:** Send subsequent email to those programs with responsive records with next steps. - Advise program areas to stand down on gathering records. **Note:** CFOI will advise GPEB - whether client wishes to continue, client wishes to change scope of request and or client does not wish to continue with request - FOIOTL will send to OPS – ED for review and approval. - Once return will send to CFOI.

DAY 2 TO 12	Compiling Records	FOIC & FOIOTL	Wil: **FOIC If no responsive records advise FOIOTL by due date:** - Complete Call for Records form (Section 3, 5 and 7) - Send to FOIOTL for review via Eapprovals – need to change approval route in EDRMS). - FOIOTL will send to OPS ED via Eapprovals and OPS ED will send back to FOIOTL to send completed CFR to CFOI- Holly Skogstad **If PA has RR - Under 3 hours** – PA has gathered records and provided their harms/concerns by using the Harms cheat sheet by due date and placed RR in restricted drive: - **In addition**: Program needs to identify any concerns with publishing records on Open Information Website. - complete Call for Records form (Section3, 5, 6A and 6B and 7) - Send to FOIOTL for review via Eapprovals – need to change approval route in EDRMS). - FOIOTL will send to OPS ED who will review and send CFR and RR's to CFOI
Day 13 - 21	CFOI will review and send to IAO	IAO	Will: - Review records and determine harms and sever records. - Produce a Redline document of responsive records. - Produce Approval form for Branch and or Ministry. - Produce Letter to client. -
Day 22-23	CFOI will send IAO Redline package to branch	FOIC & FOIOTL	FOIC Will: - Save all documents noted above from Eapproval to working folder on "J" drive working folder in corresponding folder identified as RL sub folder. - Update IAO signoff form with names of individuals involved in review (ED's) and save to Eapproval and J drive. Delete empty IAO signoff document from Eapprovals. - **Note**: We should never see the applicant's name, email, or address on the response letter. Advise FOIOTL if you see this. - Send redline and IAO supporting documents to FOIOTL for review. FOITL will: - Review redline and then send to ED's for review. - Send to Program Area ED's requesting they review redline and identify any concerns to FRU. - **Note:** Possibility – Supervisor will liaison with PSSG CFOI if PA's identify concerns with redline. IAO may be contacted with any further concerns/harms identified by Program. - IAO may need to update and produce new Redline and signoff form.

Day 24-25	Review of Redline document	ED's	Will: - Review redlines to ensure harms are identified and captured. - If program area has concerns, they must advise FOIOTL - FOI Supervisor so package can go back to IAO via CFOI for review and possible revisions. - No concerns with redline, forward to next person in approval route. **Note:** Possible delay in not meeting deadline.
Day 26 - 27	Redline package sent to ADM via E-Approvals	ADMO	Will: - Executive Co-Ordinator/Executive Assistant will forward to ADM to review. - ADM approves sends back to Executive Coordinator/Executive Assistant - Ex Co-ordinator/Executive Assistant will send back to FOI TL for processing and applying signatures to IAO approval form. **Note:** In some cases, a redline may need to be returned to IAO for further revisions if changes are required.
Day 30 - 31	Close file	FOIOTL	Will: - Complete FOI file - Add signatures of all involved to signoff form and upload to Eapproval and ensure final version saved in J drive corresponding RL folder. - Send to CFOI – Holly Skogstad to advise ADM has signed off on FOI. - **Note:** If ADM has any special instructions or comments ensure you note the comments in Eapproval for Holly. - Print off Eapproval History report and save to corresponding folder on J drive. - Change name of FOI to completed but only move to completed folder once Holly has advised FOI and been signed off and completed by DM. **(Note:** If request was for Proactive Release we will not hear back from CFOI. Closed folder.

From:	McClung, Melinda J FIN:EX
To:	CMIM-Community of Ministry Information Managers
Subject:	FW: IMML Meeting Follow-Up - Redundant Source Information Destructions
Date:	February 8, 2023 10:25:42 AM
Attachments:	image001.png

FYI - Formal direction indicating Ministries can authorize the destruction of redundant source records, including those that are SR and FR (with some exceptions).

Cheers,
Melinda

Melinda McClung *(she/her)*
Senior Data Architect
Information Management Branch, Corporate Services Division
Ministry of Finance
Phone: 778-974-3421
Office Hours: M/W/F 8:30-3:45; **T/Th** 8:30-5:00

From: Teo, HB FIN:EX <HB.Teo@gov.bc.ca>
Sent: February 8, 2023 10:12 AM
To: Peters, Jennifer L FIN:EX <Jennifer.L.Peters@gov.bc.ca>
Cc: McClung, Melinda J FIN:EX <Melinda.McClung@gov.bc.ca>; Lawes, Tamara FIN:EX <Tamara.Lawes@gov.bc.ca>
Subject: FW: IMML Meeting Follow-Up - Redundant Source Information Destructions

Please note, thanks.

HB

From: McKamey, Kristy CITZ:EX <Kristy.McKamey@gov.bc.ca> **On Behalf Of** Lowe, Charmaine CITZ:EX
Sent: February 8, 2023 9:55 AM
To: CITZ Information Management Ministry Leads <INFOMMLD@Victoria1.gov.bc.ca>
Cc: CITZ IMML Admin <IMMLADMN@Victoria1.gov.bc.ca>
Subject: IMML Meeting Follow-Up - Redundant Source Information Destructions

Dear Information Management Ministry Leads,

This is a follow up to the February 1st IMML meeting regarding the topic of streamlining approvals for redundant source records. The most common method of duplicating records is through digitization. Processes to date have required that public sector bodies request Government Records Service (GRS) approval to destroy the redundant sources records, as well as the need for a GRS archivist to appraise all the redundant source records prior to destruction.

Effective immediately, the heads of public bodies (or their delegates) that are subject to the Information Management Act (IMA) may authorize the destruction of all redundant source information, including selective retention, full retention, scheduled and unscheduled records. Please note that some very exceptional records require special attention, such as original maps, designs, drawings, or artwork, or containing unique physical elements (e.g., seals, embossing). Public bodies are required to seek appraisal and approval from GRS to destroy these types of records only.

Please ensure you are adhering to relevant policies and standards for these activities, including the Digitizing Government Information Standard and the Redundant Source Information Schedule. You must ensure that the replacement copies are authoritative copies that are produced using a defensible process, according to these standards.

The IMA seeks to streamline and modernize government's overall approach to information management. This direction for redundant source information aligns with one of the cornerstones of the IMA, which is the requirement for ministries to digitize information in preparation for the digital archives.

If you have any questions, please contact Emilie Hillier, Executive Director of the Government Records Service at Emilie.Hillier@gov.bc.ca.

Best regards,

Charmaine Lowe
Assistant Deputy Minister, Corporate Information & Records Management Office
Chief Records Officer

From: Butler, Sylvia GPEB:EX
To: Dickson, Brandy GPEB:EX
Subject: FW: Announcement - IAO"s Preprocessing and Deduplicating Service is going live
Date: February 24, 2021 4:13:00 PM
Attachments: G - Call for Records form.docx

FYI

Yours truly,

Sylvia Butler

FOI and Records Lead| Gaming Enforcement and Policy Branch |*3rd Floor, 910 Government Street*
Victoria, BC V8W 9N1 |Telephone: 778-698-5544

For any FOI inquiries please email GPEB's FOI email box (GPEB.FOIManagement@gov.bc.ca).

For any EDRMS access authorizations and or records questions, please email GPEB's Record Management mailbox (GPEB_RecordsManagement@gov.bc.ca).

From: Nisbet, Justine CITZ:EX <Justine.Nisbet@gov.bc.ca>
Sent: Thursday, January 21, 2021 4:03 PM
To: AG PSSG FOI AG:EX <AGPSSG.FOI@gov.bc.ca>; Di Georgio, Alexis AG:EX <Alexis.DiGeorgio@gov.bc.ca>; Pearson, Barbera AG:EX <Barbera.Pearson@gov.bc.ca>; Blakesley, Nicki AG:EX <Nicki.Blakesley@gov.bc.ca>; Genzale, Morgan AG:EX <Morgan.Genzale@gov.bc.ca>; Blaseckie, Rachael AG:EX <Rachael.Blaseckie@gov.bc.ca>; HOLD - 201123 - Kendall, Janelle AG:EX <Janelle.Kendall@gov.bc.ca>; AG LSB FOI Requests AG:EX <JAGLSBFOIRequests@gov.bc.ca>; Lapierre, Sylvain AG:EX <Sylvain.Lapierre@gov.bc.ca>; Marchenski, Marcia AG:EX <Marcia.Marchenski@gov.bc.ca>; Hata, Rie GPEB:EX <Rie.Hata@gov.bc.ca>; McLaughlin, Christine AG:EX <Christine.McLaughlin@gov.bc.ca>; LCRB FOI LCRB, LCRB LCRB:EX <LCLB.FOI@gov.bc.ca>; LDB Info Privacy and Access Services LDB:EX <IPAserv@bcldb.com>; GPEB FOI Management GPEB:EX <GPEB.FOIManagement@gov.bc.ca>; Boychuk, Elizabeth AG:EX <Elizabeth.Boychuk@gov.bc.ca>; Hunt, Charlotte PSSG:EX <Charlotte.Hunt@gov.bc.ca>; D'Argis, Krista PSSG:EX <Krista.DArgis@gov.bc.ca>; Bertrand, Alicia PSSG:EX <Alicia.Bertrand@gov.bc.ca>; Cherry, Don PSSG:EX <Don.Cherry@gov.bc.ca>; BCCS FOI Inbox PSSG:EX <BCCSFOI.Inbox@gov.bc.ca>; Sidhu, Tej PSSG:EX <Tej.Sidhu@gov.bc.ca>; EMBC Freedom Of Information EMBC:EX <EMBCFOI@gov.bc.ca>; Brown, Tom G EMBC:EX <Tom.Brown@gov.bc.ca>; Roe, Sandra EMBC:EX <Sandra.Roe@gov.bc.ca>; Sojonky-Gallagher, Kali PSSG:EX <Kali.SojonkyGallagher@gov.bc.ca>; Madson, Heather PSSG:EX <Heather.Madson@gov.bc.ca>; Harrison, Shanelle PSSG:EX <Shanelle.Harrison@gov.bc.ca>; Ward, Jessica PSSG:EX <Jessica.Ward@gov.bc.ca>; SG Civil Forfeiture Office SG:EX <CivilFO@gov.bc.ca>; Milne, Lauren PSSG:EX <Lauren.Milne@gov.bc.ca>; Meseyton, Robert PSSG:EX <Robert.Meseyton@gov.bc.ca>; PSSG PSD FOI PSSG:EX <PSD.FOI@gov.bc.ca>; McLachlin, Jessica PSSG:EX <Jessica.McLachlin@gov.bc.ca>; Birmingham, Lauren PSSG:EX <Lauren.Birmingham@gov.bc.ca>; Fong, Tiffany PSSG:EX <Tiffany.Fong@gov.bc.ca>; Lai, Teresa PSSG:EX <Teresa.Lai@gov.bc.ca>; Hunter, Shannon PSSG:EX <Shannon.Hunter@gov.bc.ca>; HLTH

FOI Operations HLTH:EX <HLTH.FOIOperations@gov.bc.ca>; Shust, Susan D HLTH:EX <Susan.Shust@gov.bc.ca>; Casanova, Tamara MMHA:EX <Tamara.Casanova@gov.bc.ca>
Cc: Andrews, Arielle CITZ:EX <Arielle.Andrews@gov.bc.ca>; Foster, Anita CITZ:EX <Anita.Foster@gov.bc.ca>
Subject: RE: Announcement - IAO's Preprocessing and Deduplicating Service is going live

Good Afternoon all,

As required to properly support the rollout of our new service, and as mentioned on the first two of the three scheduled MS Teams drop-in Q&A sessions, IAO has updated our call for records form (see attached). You should start seeing this new form on new calls for records shortly.

Thanks,

Justine Nisbet, Manager
Justice Social Team
Health & Mental Health Team

From: Nisbet, Justine CITZ:EX
Sent: January 13, 2021 6:14 PM
To: AG PSSG FOI AG:EX ; Di Georgio, Alexis AG:EX ; Pearson, Barbera AG:EX ; Blakesley, Nicki AG:EX ; Genzale, Morgan AG:EX ; Blaseckie, Rachael AG:EX ; HOLD - 201123 - Kendall, Janelle AG:EX ; AG LSB FOI Requests AG:EX ; Lapierre, Sylvain AG:EX ; Marchenski, Marcia AG:EX ; 'Hata, Rie AG:EX' ; McLaughlin, Christine AG:EX ; LCRB FOI LCRB, LCRB LCRB:EX ; LDB Info Privacy and Access Services LDB:EX ; GPEB FOI Management GPEB:EX ; Boychuk, Elizabeth AG:EX ; Hunt, Charlotte PSSG:EX ; D'Argis, Krista PSSG:EX ; Bertrand, Alicia PSSG:EX ; Cherry, Don PSSG:EX ; BCCS FOI Inbox PSSG:EX ; Sidhu, Tej PSSG:EX ; EMBC Freedom Of Information EMBC:EX ; Brown, Tom G EMBC:EX ; Roe, Sandra EMBC:EX ; Sojonky-Gallagher, Kali PSSG:EX ; Madson, Heather PSSG:EX ; Harrison, Shanelle PSSG:EX ; Ward, Jessica PSSG:EX ; SG Civil Forfeiture Office SG:EX ; Milne, Lauren PSSG:EX ; Meseyton, Robert PSSG:EX ; PSSG PSD FOI PSSG:EX ; McLachlin, Jessica PSSG:EX ; Birmingham, Lauren PSSG:EX ; Fong, Tiffany PSSG:EX ; Lai, Teresa PSSG:EX ; Hunter, Shannon PSSG:EX ; HLTH FOI Operations HLTH:EX ; Shust, Susan D HLTH:EX ; Casanova, Tamara MMHA:EX
Cc: Andrews, Arielle CITZ:EX ; Foster, Anita CITZ:EX
Subject: FW: Announcement - IAO's Preprocessing and Deduplicating Service is going live
Importance: High

Hello Everyone,

I'm very excited to share some important and exciting changes that IAO is implementing to improve our FOI services to you. I hope I have captured all of our clients contacts, please let me know if I've missed anyone or feel free to forward this on as you see fit.

You are encouraged to attend the info sessions set up (see attached) but please know you can reach out to me directly if you have any questions or concerns.

Kind Regards,

Justine Nisbet, Manager
Justice Social Team
Health & Mental Health Team

From: Ghag, Kris CITZ:EX <Kris.Ghag@gov.bc.ca>
Sent: January 13, 2021 3:54 PM
To: Appleton, Natalie CITZ:EX <Natalie.Appleton@gov.bc.ca>; Bejcek, Ken CITZ:EX <Ken.Bejcek@gov.bc.ca>; Elbahir, Cindy CITZ:EX <Cindy.Elbahir@gov.bc.ca>; Kane, Meghan M CITZ:EX <Meghan.Kane@gov.bc.ca>; Nisbet, Justine CITZ:EX <Justine.Nisbet@gov.bc.ca>; Onciul, Jamie CITZ:EX <Jamie.Onciul@gov.bc.ca>; Prodan, Matthew CITZ:EX <Matthew.Prodan@gov.bc.ca>
Cc: Hoskins, Chad CITZ:EX <Chad.Hoskins@gov.bc.ca>; Kukucska, Cindy L CITZ:EX <Cindy.Kukucska@gov.bc.ca>
Subject: Announcement - IAO's Preprocessing and Deduplicating Service is going live

Hi Managers,

As discussed, please share this important and exciting announcement with all of your FOI client contacts.

ANNOUNCEMENT: As of January 18, 2021, IAO is offering our new preprocessing and deduplicating service to all ministries!

Background:
We've all seen and felt over the past few years how the increase in FOI request volumes and subsequent increase in pages produced in response to FOI requests has had very real operational impacts on all of government.

Benefits of the new preprocessing and deduplicating service:
For context, over the last three complete fiscal years IAO has processed and responded to nearly 35,000 FOI requests, which has required a line-by-line review of approximately 5.5 million pages of records. We believe, with a high degree of confidence, that upwards of 10% of those pages were either duplicate records or redundant email chains (i.e. where only the most inclusive email in the chain could have been provided in order to satisfy the request). This means ***over half a million*** pages of records that added no extra value to the applicant were reviewed by IAO to make disclosure recommendations and by ministries for harms assessments and final approvals. Until now, removing duplicate records has been a highly manual and administratively burdensome process. Not removing duplicate records increases the time required to process a request and also increases the risk of inconsistent severing due to human error.

What will our new service do?

- your program areas will be able to provide records in response to FOI requests with less effort required to review, sort, and compile them;
- the various reviewers for harms or approvals will be able to get more time back in their already

busy days, as the response packages are reduced in size due to elimination of duplicate records and redundant email threads; and,
- the risk of inadvertent disclosure of sensitive information that repeats throughout a response package will be significantly reduced.

The new preprocessing and deduplication service allows IAO to:
1. Identify, match and remove all (exact) duplicate records;
2. Identify email threads and remove all redundant email chains;
3. Sort all files chronologically;
4. Burst and organize emails so that attachments stay with their parent email; and,
5. Export all files into a single PDF.

What we are asking you to do:
IAO has recently completed a pilot implementation with the Economy Sector ministries (see details below) and the only change for clients is to provide responsive records to IAO, via the normal process, in native format (e.g., just drag and drop the .msg files for emails into your shared drive) rather than converting them to pdf (i.e. we'd like to respectfully ask that you do less work compiling the records).

Pilot result details:
Over the course of a multi-month pilot with the Economy Sector, IAO has been able to determine that this service can be successfully implemented for all of our clients (as long as you are able to provide files in native format) and has been able to further refine and streamline our processes. The average file size processed during the pilot was over 700 pages and the average reduction in file size was approximately 16% - with wide variation depending on the type of request and the types of responsive records. We also determined that this process can be very effective in stripping attachments from emails (e.g. where a request specifically excludes them). Feedback received from a stakeholder survey suggests that program areas considered it to be more efficient than the previous process, with no significant delays and a high satisfaction rating.

How much time can be saved:
The largest file processed during the pilot project started with 14,550 pages of records. After deduplication, only 10,508 pages remained. This 4,000+ page, or 28%, reduction took a total of 90 minutes for IAO to complete. The alternatively, highly manual and administratively burdensome process would have taken the client contacts at least a week and would be subject to human error.

Next steps:
- Effective January 18th, please start sending native files to IAO in response to a call for records.
- Please continue to use your current process of sending files to IAO's Flex Team via the FileShare drive that has been setup for you. If for any reason you are not currently using a FileShare drive, please reach out to the Flex Team and we will set one up for you.
- Once the records have been preprocessed/deduplicated, a single pdf will be returned to you for the purposes of providing a harms assessment.
- As IAO will already have a copy of the entire records package, work may begin on sending out consultations or in determining severing that is dependent on content rather than context or

where context is obvious from the records themselves.

- Please note that the *Fee Estimate Guideline for Electronic Records* document has been updated to reflect that, for the preparation of electronic files in response to FOI requests, IAO will only require an approximate count of the number of files or number of emails in order to assess fees based on the time required for preparation.

More questions?
IAO, with some assistance from our pilot partners in the Economy Sector, have created the *Deduplication Service FAQ* document to address questions that we anticipate that you will have. Additionally, IAO will be offering three MS Teams drop-in q & a sessions for questions that have not been addressed in the FAQ. These will be held on January 15th, 20th, and 27th and invitations for each of these sessions are attached.

If you'd like any assistance briefing your senior executive on the anticipated benefits of this service, the results of our pilot project with the Economy Sector, or any other aspect of this service, we'd be happy to support you and make ourselves available to them as well.

Thanks again and we're looking forward to working with you to make FOI easier for everyone.

Kris Ghag
Senior Director, Access and Open Information
Information Access Operations **|** Corporate Information and Records Management Office
Ph: 250 387-9801 **|** ***e:*** **Kris.Ghag@gov.bc.ca** **|** ***m:*** PO Box 9569, Stn Prov Gov, Victoria BC V8W 9K1

MODULE 7E – DESTRUCTION REQUESTS OF PHYSICAL FOLDERS IN EDRMS

Role: Information Worker - FOI & Records Management Unit - FRU

Resource:

grslearning.im.gov.bc.ca/ContentManager/Disposition/applying_for_an_RDA_number/

Below are links various Information Aids on the Government Records Services website:

Records Management - Province of British Columbia (gov.bc.ca)

Appropriate Information Destruction - Province of British Columbia (gov.bc.ca)

Digitizing - Province of British Columbia (gov.bc.ca)

EDRMS Content Manager Guides - Province of British Columbia (gov.bc.ca)

Government Archives - Province of British Columbia

Information Schedules - Province of British Columbia (gov.bc.ca)

Records Management Guides and Learning - Province of British Columbia (gov.bc.ca)

Records Management Systems - Province of British Columbia (gov.bc.ca)

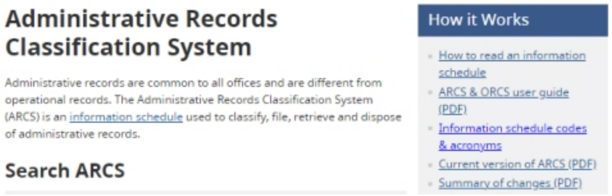
Physical Records Transfer & Offsite Storage - Province of British Columbia (gov.bc.ca)

Overview - Physical Records on site and GRS Warehouse facilities – destruction process:

Physical Records that are on site and physical records in GRS Storage facilities and that have met the end of their retention lifecycle under an approved schedule with a DE for the final disposition can be processed for on-site destruction and or direction to GRS to remove hold so that records can be destroyed at offsite facility.

Government has a responsibility to manage records and is mandated under the *Information Management Act* and regulations and various supporting resources and guidelines that provide standard procedures for all government offices. In it important to understand the lifecycle of a record.

Link to ARCS & ORCS user guide: Administrative Records Classification System - Province of British Columbia (gov.bc.ca)



Administrative Records Classification System

Administrative records are common to all offices and are different from operational records. The Administrative Records Classification System (ARCS) is an information schedule used to classify, file, retrieve and dispose of administrative records.

Search ARCS

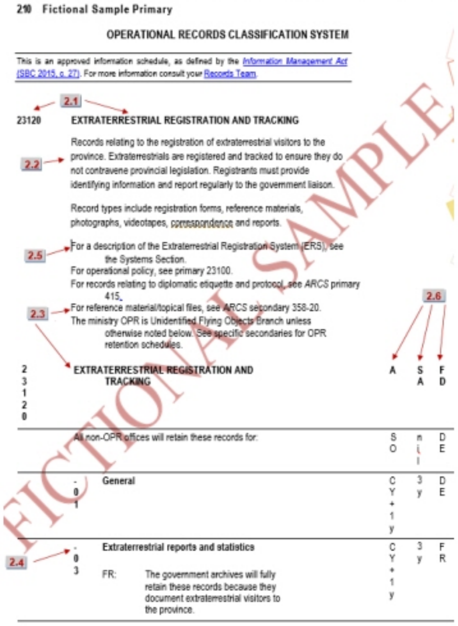
How it Works

- How to read an information schedule
- ARCS & ORCS user guide (PDF)
- Information schedule codes & acronyms
- Current version of ARCS (PDF)
- Summary of changes (PDF)

Key to Information Schedule Codes and Acronyms

Information Schedule titles System	***ARCS*** = *Administrative Records Classification* ***ORCS*** = *Operational Records Classification System*
Office information	**OPR** = Office of Primary Responsibility
Records life cycle	**A** = Active **SA** = Semi-active **FD** = Final Disposition
Active and semi-active period codes	**CY** = Calendar Year **FY** = Fiscal Year **NA** = Not Applicable **SO** = Superseded or Obsolete **w** = week **m** = month **y** = year
Final disposition categories	**DE** = Destruction **FR** = Full Retention **SR** = Selective Retention **OD** = Other Disposition **NA** = Not Applicable
Special flags Privacy	**FOI** = Freedom of Information/Protection of **PIB** = Personal Information Bank **VR** = Vital Records

Sample ORCs schedule noted below - In the fictional sample primary, extraterrestrial reports, and statistics (secondary -03) are active for the calendar year (CY) of their receipt or creation, plus one more year.



210 Fictional Sample Primary

OPERATIONAL RECORDS CLASSIFICATION SYSTEM

This is an approved information schedule, as defined by the *Information Management Act* (SBC 2015, c. 27). For more information consult your Records Team.

23120 **EXTRATERRESTRIAL REGISTRATION AND TRACKING**

Records relating to the registration of extraterrestrial visitors to the province. Extraterrestrials are registered and tracked to ensure they do not contravene provincial legislation. Registrants must provide identifying information and report regularly to the government liaison.

Record types include registration forms, reference materials, photographs, videotapes, correspondence and reports.

For a description of the Extraterrestrial Registration System (ERS), see the Systems Section.
For operational policy, see primary 23100.
For records relating to diplomatic etiquette and protocol, see *ARCS* primary 415.
For reference material/topical files, see *ARCS* secondary 358-20.
The ministry OPR is Unidentified Flying Objects Branch unless otherwise noted below. See specific secondaries for OPR retention schedules.

		A	SA	FD
23120	**EXTRATERRESTRIAL REGISTRATION AND TRACKING**			
	All non-OPR offices will retain these records for:	SO	nil	DE
-01	**General**	CY+1y	3y	DE
-03	**Extraterrestrial reports and statistics** FR: The government archives will fully retain these records because they document extraterrestrial visitors to the province.	CY+1y	3y	FR

GRS – Administrative Record Schedule – (ARCS) On – line resource:

https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/records-management/information-schedules/arcs

GRS – Operational Record Schedule (ORCS) – On – line resource:

Operational Records Classification Systems - Province of British Columbia (gov.bc.ca)

Various branch/ministry ORCS are listed alphabetically - Gaming Policy and Enforcement Branch can be found under G.

GRS – SPECIAL SCHEDULES (EXECUTIVE RECORDS):

Executive Records (schedule 102906) - Province of British Columbia (gov.bc.ca)

Resources available:

How to complete form below is described in the following video – which is high level resource, it does not speak to branch procedures that have been created:

grslearning.im.gov.bc.ca/ContentManager/Disposition/Course_Menu/index.html

January 1, 2023 – Government Records Services announced they are returning the responsibility and management of the destruction of records and redundant records to the Ministries.

This module represents a living document that will be updated as we work through each type of record noted below:

1) Physical Records on site (Administrative and Operational records)
2) Physical Records in government storage warehouses (60-day notifications from GRS)
3) EDRMS records
4) Records on LAN drives
5) Records within Outlook email system
6) Other – (media files or other formats of records)

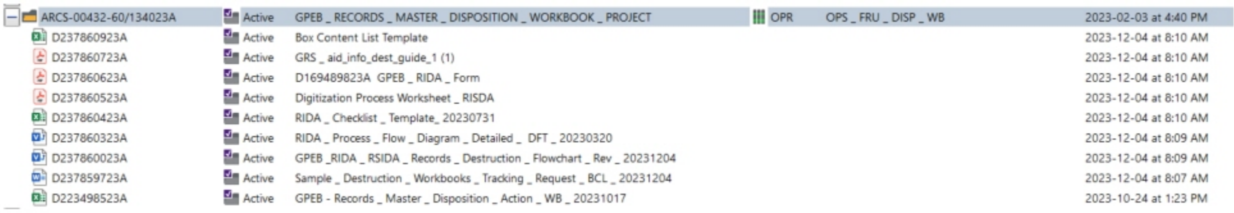
This Module covers the 1 & 2 from record types noted above: processes:

1) Processing on site destruction of physical records

2) 60 Day notification – under construction.

Creating On-site Destruction of Physical Records Request:

See flowcharts for this process within GPEB Master Disposition folder in EDRMS:



ARCS-00432-60/134023A	Active	GPEB _ RECORDS _ MASTER _ DISPOSITION _ WORKBOOK _ PROJECT	OPR	OPS _ FRU _ DISP _ WB	2023-02-03 at 4:40 PM
D237860923A	Active	Box Content List Template			2023-12-04 at 8:10 AM
D237860723A	Active	GRS _ aid_info_dest_guide_1 (1)			2023-12-04 at 8:10 AM
D237860623A	Active	D169489823A GPEB _ RIDA _ Form			2023-12-04 at 8:10 AM
D237860523A	Active	Digitization Process Worksheet _ RISDA			2023-12-04 at 8:10 AM
D237860423A	Active	RIDA _ Checklist _ Template_ 20230731			2023-12-04 at 8:10 AM
D237860323A	Active	RIDA _ Process _ Flow _ Diagram _ Detailed _ DFT _ 20230320			2023-12-04 at 8:09 AM
D237860023A	Active	GPEB _RIDA _ RSIDA _ Records _ Destruction _ Flowchart _ Rev _ 20231204			2023-12-04 at 8:09 AM
D237859723A	Active	Sample _ Destruction _ Workbooks _ Tracking _ Request _ BCL _ 20231204			2023-12-04 at 8:07 AM
D223498523A	Active	GPEB - Records _ Master _ Disposition _ Action _ WB _ 20231017			2023-10-24 at 1:23 PM

Step 1) Request for Information Destruction Authorization (RIDA):

FOI and Records Management unit will complete and manage the RIDA or RISDA for on-site destruction for the branch.

FOI and Records Management Team Lead (For all office locations)

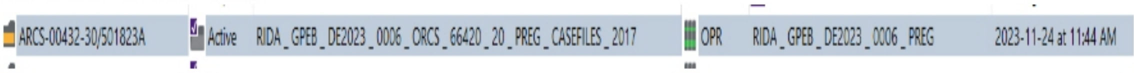
FOI and Records Management Co-ordinator (For all office locations)

Roles and responsibilities within process:

FOI and Records Management Officer – Team Lead:

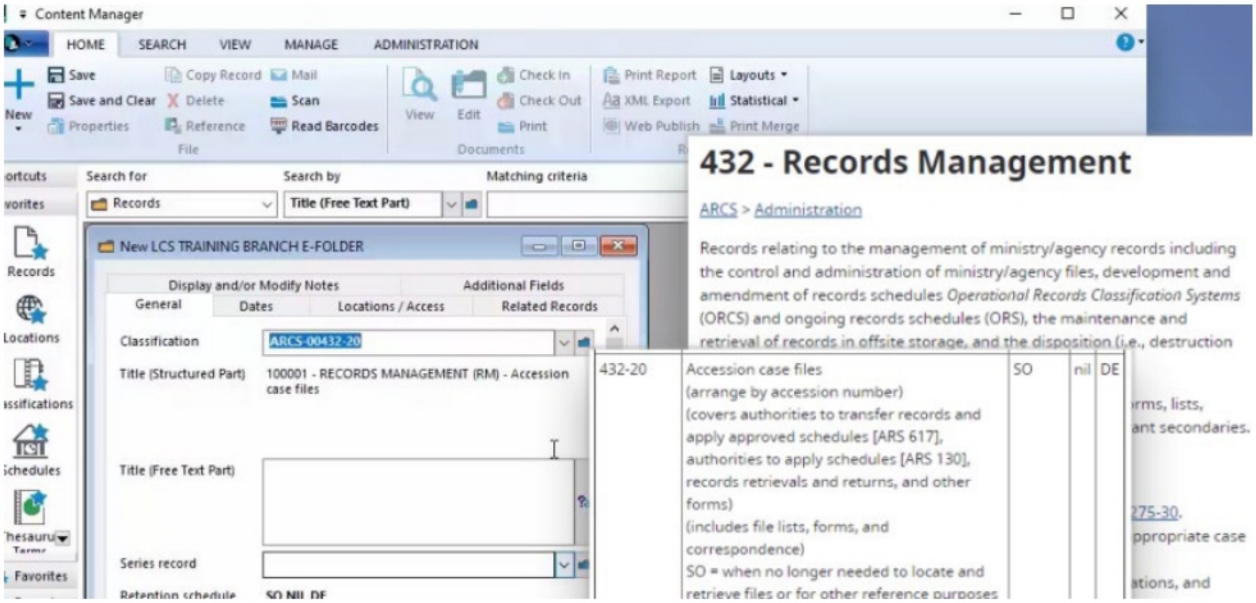
Identifies records to be reviewed and classified and prepared for destruction.
Create folder in EDRMS.

e.g.,



ARCS-00432-30/501823A Active RIDA_GPEB_DE2023_0006_ORCS_66420_20_PREG_CASEFILES_2017 OPR RIDA_GPEB_DE2023_0006_PREG 2023-11-24 at 11:44 AM

Creates E folder in EDRMS under classification ARCs-00432-30



New LCS TRAINING BRANCH E-FOLDER

Display and/or Modify Notes | Additional Fields
General | Dates | Locations / Access | Related Records

Classification: ARCS-00432-20

Title (Structured Part): 100001 - RECORDS MANAGEMENT (RM) - Accession case files

Title (Free Text Part):

Series record:

Retention schedule: SO NIL DE

432 - Records Management

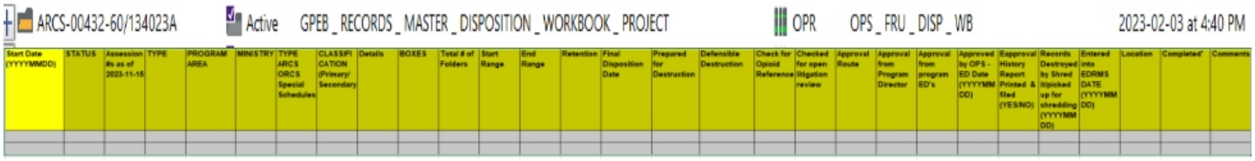
ARCS > Administration

Records relating to the management of ministry/agency records including the control and administration of ministry/agency files, development and amendment of records schedules *Operational Records Classification Systems* (ORCS) and ongoing records schedules (ORS), the maintenance and retrieval of records in offsite storage, and the disposition (i.e., destruction

432-20	Accession case files (arrange by accession number) (covers authorities to transfer records and apply approved schedules [ARS 617], authorities to apply schedules [ARS 130], records retrievals and returns, and other forms) (includes file lists, forms, and correspondence) SO = when no longer needed to locate and retrieve files or for other reference purposes	SO	nil	DE

rms, lists,
ant secondaries.
275-30.
ppropriate case
ations, and

Creates a new entry to the GPEB Master Disposition List



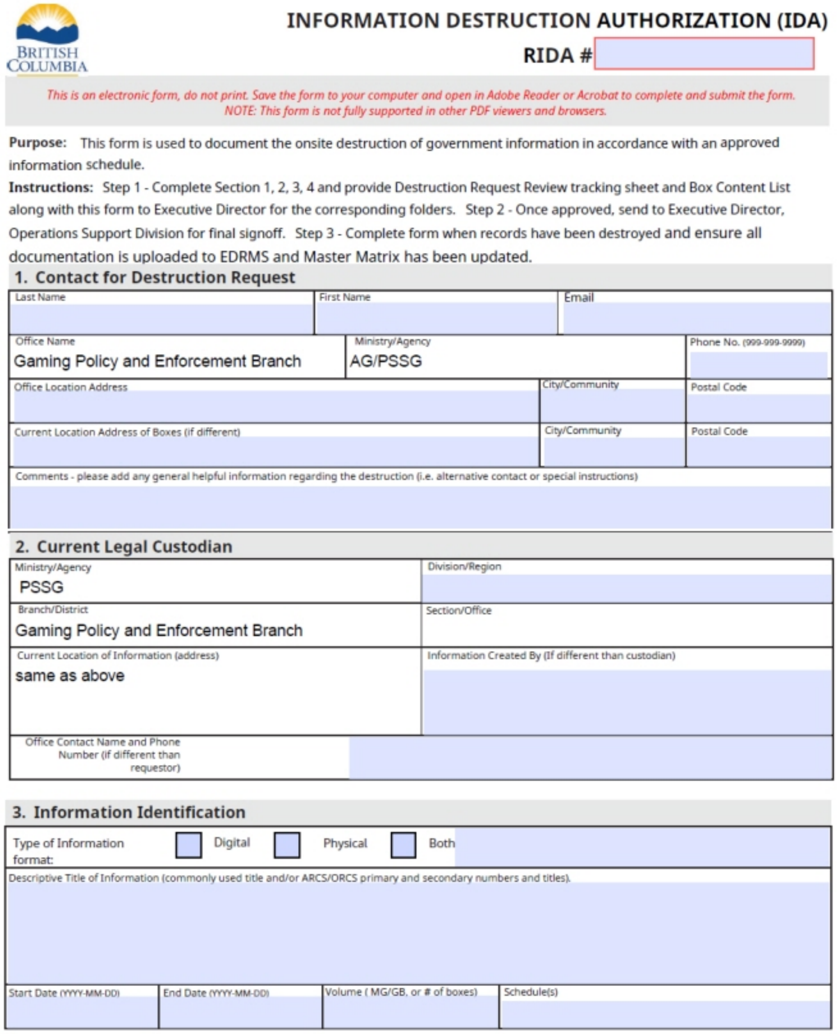
ARCS-00432-60/134023A Active GPEB_RECORDS_MASTER_DISPOSITION_WORKBOOK_PROJECT OPR OPS_FRU_DISP_WB 2023-02-03 at 4:40 PM

Start Date (YYYYMMDD)	STATUS	Assession #s as of 2023-11-15	TYPE	PROGRAM AREA	MINISTRY	TYPE ARCS ORCS Special Schedules	CLASSIFICATION (Primary/ Secondary	Details	BOXES	Total # of Folders	Start Range	End Range	Retention	Final Disposition Date	Prepared for Destruction	Defensible Destruction	Check for Opioid Reference	Checked for open litigation review	Approval Route	Approval from Program Director	Approval from program ED's	Approved by OPS - ED Date (YYYYMMDD)	Eapproval History Report Printed & filed (YES/NO)	Records Destroyed by Shred it/picked up for shredding (YYYYMMDD)	Entered into EDRMS DATE (YYYYMMDD)	Location	Completed'	Comments

Meets with FOI and Records Management Co-ordinator to review.

Initiates RIDA and saves to EDRMS corresponding file.

NOTE: The form is a pdf fillable form that can be saved to working folder in EDRMS once process has been completed. All supporting documents will be filed in EDRMS under classification ARCS – 00432-30.



BRITISH COLUMBIA

INFORMATION DESTRUCTION AUTHORIZATION (IDA)

RIDA #

This is an electronic form, do not print. Save the form to your computer and open in Adobe Reader or Acrobat to complete and submit the form.
NOTE: This form is not fully supported in other PDF viewers and browsers.

Purpose: This form is used to document the onsite destruction of government information in accordance with an approved information schedule.

Instructions: Step 1 - Complete Section 1, 2, 3, 4 and provide Destruction Request Review tracking sheet and Box Content List along with this form to Executive Director for the corresponding folders. Step 2 - Once approved, send to Executive Director, Operations Support Division for final signoff. Step 3 - Complete form when records have been destroyed and ensure all documentation is uploaded to EDRMS and Master Matrix has been updated.

1. Contact for Destruction Request

Last Name:
First Name:
Email:
Office Name: Gaming Policy and Enforcement Branch
Ministry/Agency: AG/PSSG
Phone No. (999-999-9999):
Office Location Address:
City/Community:
Postal Code:
Current Location Address of Boxes (if different):
City/Community:
Postal Code:
Comments - please add any general helpful information regarding the destruction (i.e. alternative contact or special instructions):

2. Current Legal Custodian

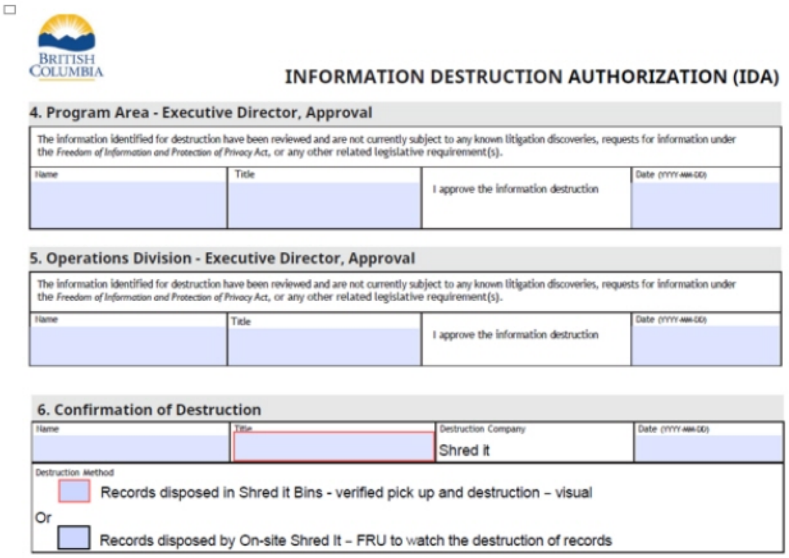
Ministry/Agency: PSSG
Division/Region:
Branch/District: Gaming Policy and Enforcement Branch
Section/Office:
Current Location of Information (address): same as above
Information Created By (If different than custodian):
Office Contact Name and Phone Number (if different than requestor):

3. Information Identification

Type of Information format: □ Digital □ Physical □ Both

Descriptive Title of Information (commonly used title and/or ARCS/ORCS primary and secondary numbers and titles).

Start Date (YYYY-MM-DD):
End Date (YYYY-MM-DD):
Volume (MG/GB, or # of boxes):
Schedule(s):



□

BRITISH COLUMBIA

INFORMATION DESTRUCTION AUTHORIZATION (IDA)

4. Program Area - Executive Director, Approval

The information identified for destruction have been reviewed and are not currently subject to any known litigation discoveries, requests for information under the *Freedom of Information and Protection of Privacy Act*, or any other related legislative requirement(s).

Name	Title	I approve the information destruction	Date (YYYY-MM-DD)

5. Operations Division - Executive Director, Approval

The information identified for destruction have been reviewed and are not currently subject to any known litigation discoveries, requests for information under the *Freedom of Information and Protection of Privacy Act*, or any other related legislative requirement(s).

Name	Title	I approve the information destruction	Date (YYYY-MM-DD)

6. Confirmation of Destruction

Name	Title	Destruction Company Shred it	Date (YYYY-MM-DD)

Destruction Method

□ Records disposed in Shred it Bins - verified pick up and destruction – visual

Or

□ Records disposed by On-site Shred It – FRU to watch the destruction of records

FOI and Records Management Co-ordinator:

Complete review and preparation- classification, system review, reviewing any issues with program area and FOI RMO Team Lead and complete box content lists for records identified for destruction.

Sends to Team Lead via Eapproval

Provides location of working documentation:

Box Content List – draft
Ensures boxes are labelled for destruction and place in holding room.

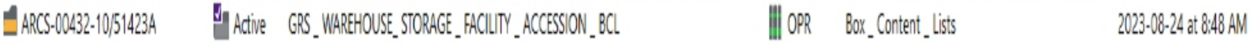
FOI and Records Management Officer – Team Lead:

Reviews box content list – quality control check

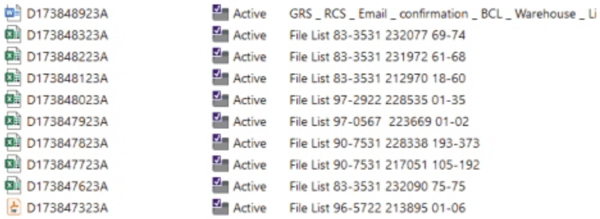
- If errors are noted – return bcl to FOI RM Coordinator for correction.
- Meet with FOI RM Coordinator to discuss issues/errors.
- FOI RM Coordinator to correct and return bcl to Team Lead
- Update RIDA in EDRMS

Once completed bcl received – revisit bcl list to ensure all errors are corrected.
Completes box content list – justification portion of box content list.
Completes RIDA in preparation for Divisional review and approval.
Updates GPEB Master Disposition list with EDRMS
Updates folder in EDRMS with semi-final documents

Adds Box content list to GPEB Master Box Content List – for all destruction requests.



ARCS-00432-10/51423A Active GRS_WAREHOUSE_STORAGE_FACILITY_ACCESSION_BCL OPR Box_Content_Lists 2023-08-24 at 8:48 AM



D173848923A	Active	GRS _ RCS _ Email _ confirmation _ BCL _ Warehouse _ Li
D173848323A	Active	File List 83-3531 232077 69-74
D173848223A	Active	File List 83-3531 231972 61-68
D173848123A	Active	File List 83-3531 212970 18-60
D173848023A	Active	File List 97-2922 228535 01-35
D173847923A	Active	File List 97-0567 223669 01-02
D173847823A	Active	File List 90-7531 228338 193-373
D173847723A	Active	File List 90-7531 217051 105-192
D173847623A	Active	File List 83-3531 232090 75-75
D173847323A	Active	File List 96-5722 213895 01-06

NOTE: Currently working on converting old historical list to OCR's PDF to enable searching on historical bcl. Whereas old excel workbooks will be added to new workbook.

Updates Eapproval with RIDA and Checklist and EDRMS reference for Directors and Executive Director to view bcl. BCL will provide not only records identified for destruction but also include reference to classification and retention period. In addition – process used to determine that records have met their retention requirements.

Request division review the Destruction checklist which includes all facets of defensible destruction, records requirements and questions that need to be answered by program areas. Executive Directors are asked to provide their approval or denial in Eapproval system and return to Team Lead within two weeks.

Sets two-week diary date.

Follows up with review with program area to answer any questions or concerns.

Executive Directors and Directors of each Division within GPEB – to review all supporting documentation:

RIDA application
Destruction Checklist (records background, defensible destruction questions, critical information review and additional questions
Box content list
Return eapproval to FOI and Records Mgmt. Officer – Team Lead

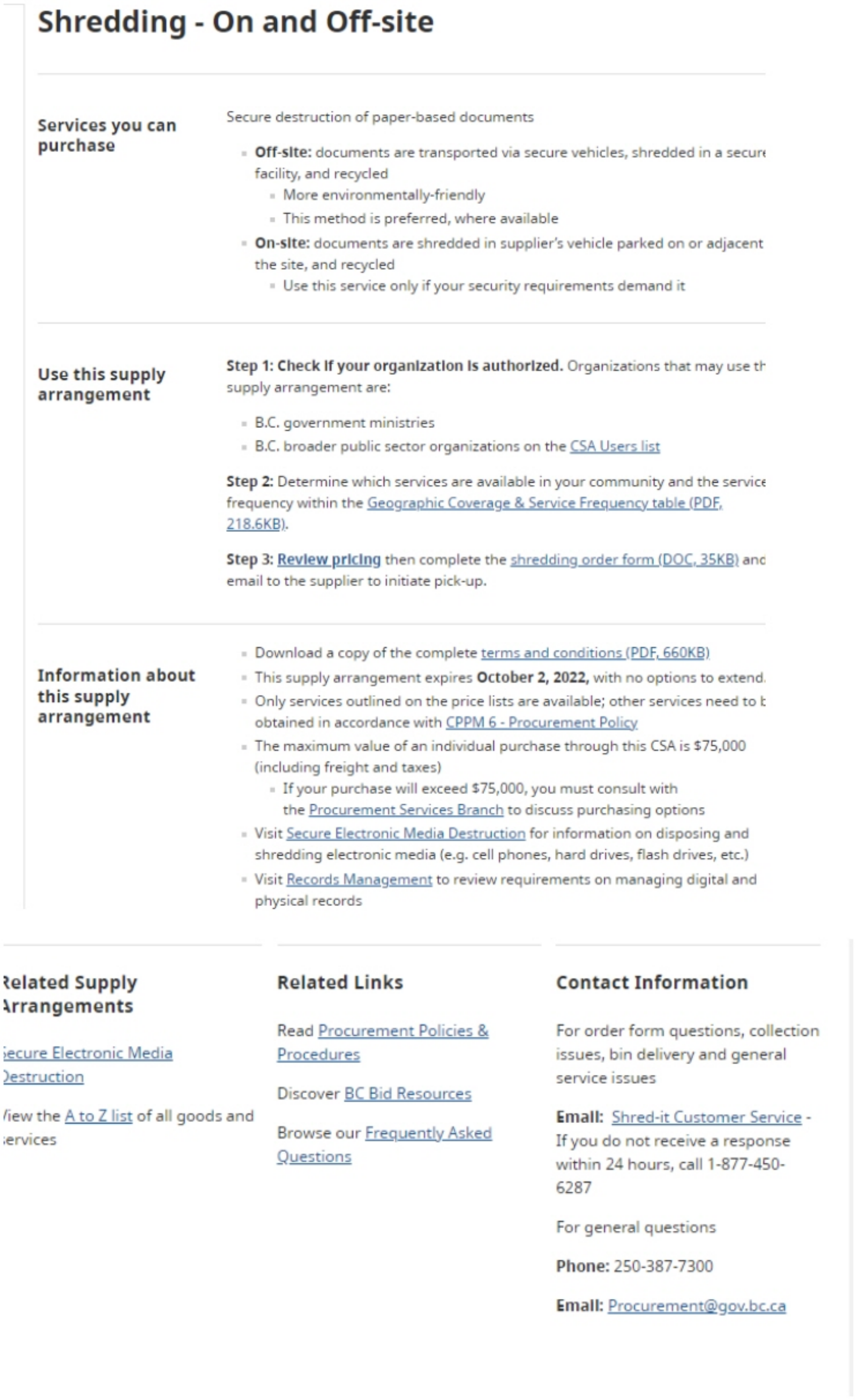
FOI _ RMTL will forward eapproval to Executive Director for final approval.
Update EDRMS and Master Disposition list

Executive Director, Operations Support Division – Final Approver – to review eapproval documents and EDRMS reference (BCL) and Director and Executive Director's comments and approval confirmation.

Return approval/questions to FOI RMO Team Lead

FOI RMO TL will finalize document or review any questions raised. If approved – updated EDRMS, Master Disposition Log, Move BCL to GPEB Master list in EDRMS and ensures all supporting material and Ehistory report is filed or updated in EDRMS.

Advise FOI RM Coordinator that records can be placed in Shred It Bins and advise Shred it driver to contact you upon arrival so that FOI RM Co-ordinator can join Shred It driver to watch records being destroyed.



Shredding - On and Off-site

Services you can purchase

Secure destruction of paper-based documents

- **Off-site:** documents are transported via secure vehicles, shredded in a secur facility, and recycled
  - More environmentally-friendly
  - This method is preferred, where available
- **On-site:** documents are shredded in supplier's vehicle parked on or adjacent the site, and recycled
  - Use this service only if your security requirements demand it

Use this supply arrangement

Step 1: Check if your organization is authorized. Organizations that may use th supply arrangement are:

- B.C. government ministries
- B.C. broader public sector organizations on the CSA Users list

Step 2: Determine which services are available in your community and the service frequency within the Geographic Coverage & Service Frequency table (PDF, 218.6KB).

Step 3: Review pricing then complete the shredding order form (DOC, 35KB) anc email to the supplier to initiate pick-up.

Information about this supply arrangement

- Download a copy of the complete terms and conditions (PDF, 660KB)
- This supply arrangement expires **October 2, 2022,** with no options to extend.
- Only services outlined on the price lists are available; other services need to b obtained in accordance with CPPM 6 - Procurement Policy
- The maximum value of an individual purchase through this CSA is $75,000 (including freight and taxes)
  - If your purchase will exceed $75,000, you must consult with the Procurement Services Branch to discuss purchasing options
- Visit Secure Electronic Media Destruction for information on disposing and shredding electronic media (e.g. cell phones, hard drives, flash drives, etc.)
- Visit Records Management to review requirements on managing digital and physical records

Related Supply Arrangements

Secure Electronic Media Destruction

View the A to Z list of all goods and services

Related Links

Read Procurement Policies & Procedures

Discover BC Bid Resources

Browse our Frequently Asked Questions

Contact Information

For order form questions, collection issues, bin delivery and general service issues

Email: Shred-it Customer Service - If you do not receive a response within 24 hours, call 1-877-450-6287

For general questions

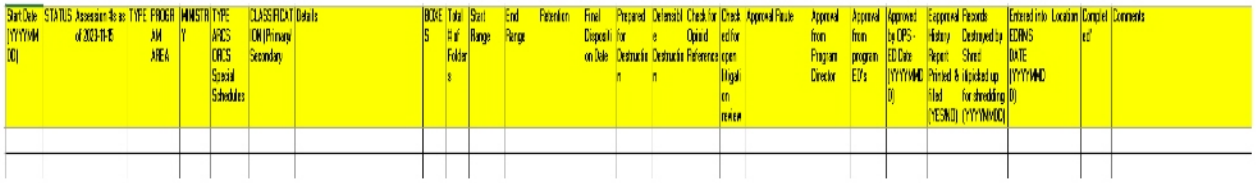
Phone: 250-387-7300

Email: Procurement@gov.bc.ca

In addition – FRU manages a master matrix of all box content lists for records that have been destroyed or sent offsite.

As well as a separate Master matrix for tracking requests, retrieval, return, destructions and 60-day notification under ARCs-432-10 in EDRMS (June 2023 - under construction).

Sample of GPEB Records Mater Disposition Workbook:



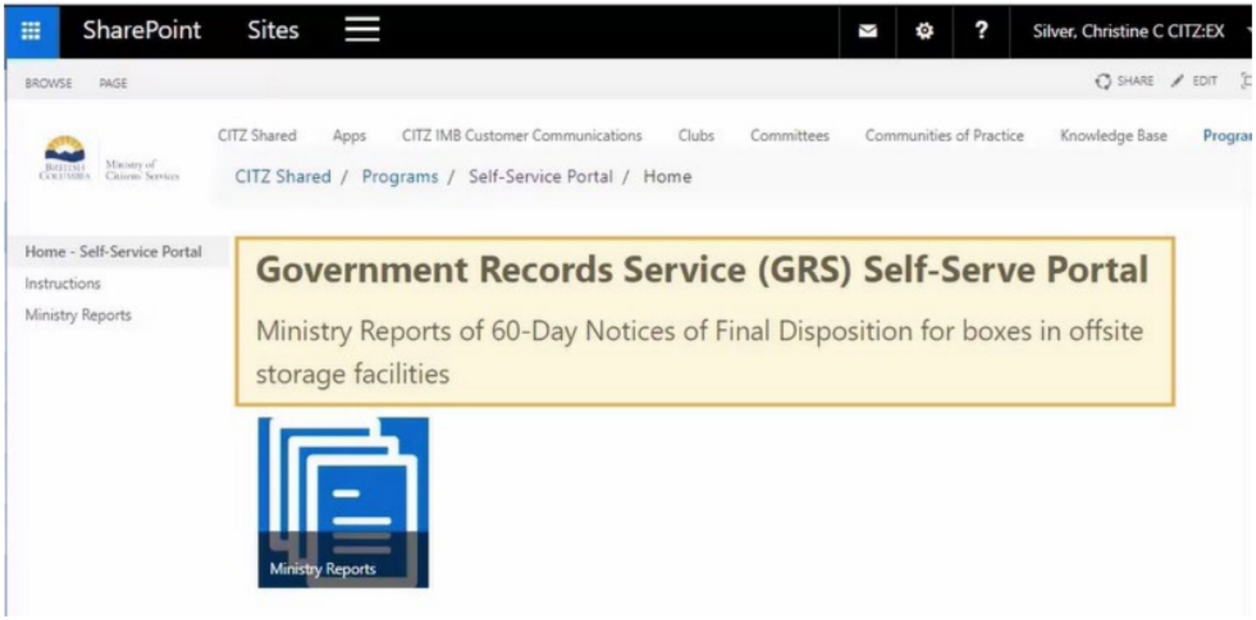
Start Date (YYYYMMDD)	STATUS	Accession #s as of 2023-11-15	TYPE	PROGRAM AREA	MINISTRY	TYPE ARCS ORCS Special Schedules	CLASSIFICATION (Primary/ Secondary	Details	BOXES	Total # of Folders	Start Range	End Range	Retention	Final Disposition Date	Prepared for Destruction	Defensible Destruction	Check for Opioid Reference	Checked for open litigation review	Approval Route	Approval from Program Director	Approval from program ED's	Approved by OPS-ED Date (YYYYMMDD)	Eapproval History Report Printed & filed (YES/NO)	Records Destroyed by Shred it/picked up for shredding (YYYYMMDD)	Entered into EDRMS DATE (YYYYMMDD)	Location	Completed?	Comments

File the final records under the corresponding folder in EDRMS.

2) 60 Day notification – under construction.

Link: grslearning.im.gov.bc.ca/RecordsManagement/AdminPractices/60_Day_Notices/

These notices are produced by GRS and placed on SharePoint site. The 60-day notices only apply to physical sent offsite to storage facility and or electronic folders that have met their lifecycle retention periods.



SharePoint
Sites
Silver, Christine C CITZ:EX
BROWSE
PAGE
SHARE
EDIT
British Columbia Ministry of Citizens' Services
CITZ Shared
Apps
CITZ IMB Customer Communications
Clubs
Committees
Communities of Practice
Knowledge Base
Progra
CITZ Shared / Programs / Self-Service Portal / Home
Home - Self-Service Portal
Instructions
Ministry Reports

Government Records Service (GRS) Self-Serve Portal

Ministry Reports of 60-Day Notices of Final Disposition for boxes in offsite storage facilities

Alerts are sent out to GPEB Records Management Unit who manages the 60-day notices.

20231101 - Currently GPEB records in GRS records storage facilities on hold while reviewing new process which will be similar in nature to the on-site destruction process. However, once reviewed and signoff have been approved, an email will be sent to GRS that hold can be removed and records can be destroyed by facility. Confirmation email from facility and GRS will be required to complete our files of destruction.

Next processes to be reviewed:

1) EDRMS records (E and P folders)
2) Records on LAN drives
3) Records within Outlook email system
4) Other – (media files or other formats of records)

GAMING POLICY AND ENFORCEMENT BRANCH
Administrative and Operational Policy Manual

Records Management

version 1.0

Updated: May 13, 2022

Version Control

Date	Version Number	Brief Description of Change	Initial

Table of Contents

GPEB Records Management

The Gaming Policy and Enforcement Branch (GPEB) is the steward of a significant amount of information and records. GPEB is responsible for managing these records pursuant to the requirements of the *Information Management Act*, as well as the directives, policies and procedures set out by the government's Corporate Information and Records Management Office (CIRMO).[1] GPEB has also developed internal policies and procedures to ensure consistent records practice within the Branch.

All GPEB employees have a role in the management of GPEB's records. This manual outlines the policies and processes that all employees should be aware of, and adhere to, in the management of the Branch's information and records.

About this Manual

GPEB employees deal with a diverse range of information and records, requiring different levels of knowledge and detail. This manual has been structured to allow users to easily identify and select the level of detail they need to meet their records management responsibilities.

- Eight sections provide an overview of what all employees need to know about:
    1. Their responsibilities in relation to records management;
    2. Day-to-day management of GPEB records;
    3. Enterprise Document Records Management System Content Manager (EDRMS);
    4. Applications and systems used in the day-to-day management of GPEB records;
    5. Handling of personal and confidential information;
    6. Freedom of Information Requests;
    7. Departing employees; and
    8. Procedures.

- Within each section, links are provided to relevant GPEB and/or government policies or guidelines. It is the employee's responsibility to familiarize themself with all policies that are relevant to the work they do and the type of records they handle.

- Where relevant, links are also provided to procedures for readers who require greater detail. A list of all procedures, including links, can be found in the final section of this manual.

[1] CIRMO falls under the mandate of the Chief Records Officer (CRO), who is responsible for all BC government's information management practices, legislation, and policies.

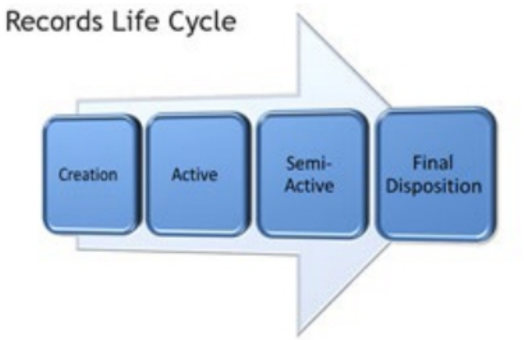
Records Management FAQs

What is a record?

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, mechanic or otherwise. Records can be in either electronic/digital or physical/paper format. GPEB's vision for records management is to become a fully electronic work environment.

What is records management and why is it important?

Records management encompasses the processes and policies that apply throughout the life cycle of records: creation and receipt; active; semi-active; and final disposition.



Records management is important for:

- Ensuring that all GPEB's key activities and decisions are documented and subsequently preserved for the requisite period of time, providing organizational history and accountability.

- Enabling timely search and retrieval of documents whenever they are required.

My position does not have specific records duties. How does this manual apply to me?

While there are some positions in GPEB dedicated to records management either in full or in part, *each GPEB employee is responsible for managing the records they create and/or receive during their day-to day work activities*. Examples include managing their emails and work notes, and ensuring all personal and confidential information is handled appropriately.

What is EDRMS?

The Enterprise Document Records Management System Content Manager (EDRMS) is government's record keeping system, used to manage records throughout their life cycle. GPEB has adopted EDRMS as its primary records repository; all non-transitory GPEB records must be filed in this system, with the exception of some operational records (e.g., investigation files) that are filed in the Gaming Online Service (GOS). In EDRMS, electronic records are captured, protected, retained, and destroyed in accordance with approved information schedules.

Who should I contact if I have any questions?

Contact GPEB.RecordsManagement@gov.bc.ca for any questions or assistance with this manual or any of the records policies.

Relevant Legislation and Policy

In the BC public sector, the management of information is governed by an integrated and complementary suite of legislation and policy, including but not limited to:

- *Information Management Act* (IMA)
  - Administrative Records Classification System (ARCS)
  - Operational Records Classification System (ORCS)
  - Special Schedules (Executive Records, Redundant Source Information, Transitory Information)
- *Freedom of Information and Protection of Privacy Act* (FOIPPA)
- *Managing Government Information Policy* (MGIP)
  - The *Recorded Information Management Manual* (RIM - in revision) details standards, processes and procedures to support IM and ministry adherence to the requirements detailed in the *Managing Government Information Policy*.
- *Core Policy and Procedures Manual* (CPPM) Chapter 12: Information Management and Information Technology Management
- Directives and guidelines issued by the Chief Records Officer (CRO) under the IMA; and
- Corporate policies, standards and strategic direction issued by government, including the:
  - *Standards of Conduct for BC Public Service Employees*
  - *Draft Principles that Guide the Province's Relationship with Indigenous Peoples*
  - *Digital Principles for the Government of British Columbia*
  - *Policies and standards issued by Office of the Chief Information Officer (OCIO)*

Acronyms & Abbreviations

The following acronyms are used in this manual. Please see the GPEB Records Master Matrix for the acronyms to be used in the naming of folders and records.

The Act – *Gaming Control Act*

ARCS – Administrative Records Classification System

CFR – Call for Records

CIRMO – Corporate Information and Records Management Office

CRO – Chief Records Officer

EDRMS – Enterprise Document Records Management System Content Manager

FOIPPA – *Freedom of Information and Protection of Privacy Act*

GOS – Gaming Online Service

GPEB – Gaming Policy and Enforcement Branch

IMA – *Information Management Act*

LAN – Local Area Network

OPR - Office of Primary Responsibility

ORCS - Operational Records Classification System

The Regulation – Gaming Control Regulation

Glossary

Administrative records – Records that are common to all offices and pertain to business functions such as facilities management, property, finance, personnel, and information systems. They also include management functions like committees, contracts, and legal activities.

Administrative Records Classification System (ARCS) – An information schedule used to classify, file, retrieve and dispose of administrative records.

Classification system – A combined records classification and scheduling system that facilitates the efficient and systematic organization, retrieval, storage, and destruction or permanent retention of the government's operational records.

Collaboration tools – Applications or software that allow multiple users to work together on projects from any location and from different devices. Examples include, but are not limited to, MS Teams, Skype, SharePoint, eApprovals, OneDrive, and OneNote.

Confidential information – Information that includes Cabinet confidences, government economic or financial information, information harmful to intergovernmental relations, and third-party business information, where the disclosure of the information would harm the third party.

Enterprise Document Records Management System Content Manager (EDRMS) – A records management system used by government and the broader public sector worldwide to manage physical and electronic records throughout their life cycle. EDRMS ensures that records are captured, protected, retained, and destroyed in accordance with approved information schedules such as the Administrative Records Classification System (ARCS) and the Operational Records Classification System (ORCS). EDRMS is the records repository approved by the BC government and used by GPEB. With the exception of some operational records (e.g., investigation files), all GPEB records that require long-term retention must be filed in EDRMS.

Gaming Online Service (GOS) – A web-based application used by applicants to submit applications and pay application fees for gaming worker registration. GOS is also an internal-facing application used by GPEB staff. Some GPEB divisions use GOS for primary intake from service providers or registrants, or throughout the investigative process for some types of investigations, where it is utilized for retaining the investigation records for future reference or connections to other potential files or individuals.

General Manager – An individual appointed by the Minister under the *Public Service Act* to be the General Manager pursuant to section 24 of the *Gaming Control Act*.

Information schedule – Information schedules ensure that government information is accessible and kept as long as needed, and that information whose value has expired is destroyed in a timely, secure manner. They serve as timetables governing the life cycle of information, and also as classification tools that place the information in the context of related records and systems.

Local Area Network (LAN) – A computer network that interconnects computers within a limited area such as government.

The Minister – The member of Cabinet who has been assigned oversight responsibility for GPEB.

Office of Primary Responsibility (OPR) – The office that has been designated the holder of the official record for the Ministry. The OPR maintains the official record to satisfy operational or administrative records related to general administration, building, equipment, financial, legal, legislative, information technology, etc.

Operational records – Records that are unique to each government ministry, branch, or broader public sector organization. They document the specific operational services of each government body. Examples of operational records for GPEB are investigative files created by the Enforcement Division or Gambling Support BC records.

Operational Records Classification System (ORCS) – An information schedule used to classify, file, retrieve and dispose of operational records.

Personal information – Recorded information about an identifiable individual other than business contact information; it includes such things as age, gender, and marital status. The *Freedom of Information and Protection of Privacy Act* (FOIPPA) sets out requirements pertaining to the collection, use and disclosure of personal information by public sector bodies.

Record – 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, mechanic or otherwise. (*Interpretation Act*, BC Laws)

Records repository – A shared filing system in which records are captured, protected, retained, and destroyed in accordance with approved information schedules. EDRMS and GOS are the records repositories for GPEB.

Transitory information – Information that is not required to support or document a government body's actions and decision-making. Transitory information is information of temporary usefulness that is only needed to complete a routine action or prepare a subsequent record (e.g., a new version). Transitory information requirements are established in the Transitory Information Schedule.

Content and context determine whether recorded information is transitory, not its format or medium. Just like other records, transitory information can exist in any format (paper or digital) and can be created and shared over a variety of media (e.g., email, social media, handwritten notes, voice mail, MS Teams, SharePoint, wikis, digital systems).

1.0 Employee Responsibilities Relating to Records Management

All GPEB employees, regardless of their position, are responsible for managing the records they create and receive in accordance with the policies and procedures set by the Corporate Information and Records Management Office (CIRMO) and/or GPEB Executive. These responsibilities are outlined in Table 1, below.

Table 1: Employee Responsibilities Relating to Records Management

EMPLOYEE RESPONSIBILITY	RELATED POLICY OR SECTION
(a) Ensuring all non-transitory records are filed in the appropriate system	• Enterprise Document Records Management System Content Manager (EDRMS)
(a) Using approved naming conventions and common classifications when creating and/or filing records	• Naming Conventions for Folders and Records Policy • GPEB Records Master Matrix •
(b) Managing emails	• Managing Government Emails Policy • Email Guide
(c) Managing work-related notes	• Employee Notes Policy
(d) Managing personal H: drives	• Managing H: Drives
(e) Ensuring proper measures are taken to protect privacy and confidentiality	• Handling of Personal and Confidential Information • Disposal of Transitory Records (shredding)
(f) Searching for records in response to Freedom of Information requests (duty to assist)	• Freedom of Information Requests
(g) Identifying and disposing of transitory and redundant records	• Identification of Transitory Information • Disposal of Transitory Records (shredding) • Redundant Records
(h) Digitizing records	• Scanning of Paper Records Policy

1.1 Working Remotely

The records management policies, processes and guidelines referenced in this manual apply to all workspaces, whether the GPEB employee is working in a government office, at home, a public space, or a mobile workspace.

- See Managing Records Outside the Office Guide
- See Online Meetings Guide

2.0 Day-to-Day Records Management for GPEB Employees

Purpose

1. Explain the records-related responsibilities that apply to all GPEB employees in their daily work.

2.1 Naming of Records and Folders

All GPEB records and folders should adhere to GPEB's naming convention policy. The organization and naming of records in a consistent manner will ensure they can be easily identified and retrieved if required at a later date. The following policies outline requirements for employees when naming folders and records:

- Naming Conventions for Folders and Records Policy

2.2 Classification of Records

All records must be classified in accordance with applicable information schedules to ensure they are retained for the appropriate length of time. The following information schedules apply to GPEB records:

1. **Administrative Records Classification System (ARCS -** Schedule 100001)
   Administrative records are common to all government offices and support business functions such as facilities management, property, finance, personnel, and information systems. ARCS also includes management functions like committees, contracts, and legal activities.
2. **GPEB's Operational Records Classification System (GPEB ORCS -** Schedule 179964)
   Operational records are unique to each government ministry, branch, or broader public sector organization; they document the specific operational services of each government body. Examples of operational records for GPEB are investigative files created by the Enforcement Division or Gambling Support BC records.
3. **Special Schedules**
   Special schedules are information schedules used to manage and schedule records that do not fit into either administrative or operational records categories. The special schedules used by GPEB are: Executive Records (Schedule 102906), Redundant Source Information (Schedule 206175), and Transitory Information (Schedule 102901).

For more information on how to classify and name GPEB records, see:

- GPEB Records Master Matrix
- Procedure Module 1A: Records Management Overview
- Procedure Module 1B: Records Management Classification Systems

2.3 Emails

Emails pertaining to the business of government are considered to be government records and as such, must be managed in accordance with all records-related legislative and policy requirements.

- See Managing Government Emails Policy

2.4 Employee Notes

Work-related notes recorded by employees are government records and as such, must be managed in accordance with all records-related legislative and policy requirements.

- See Employee Notes Policy

2.5 Identification and Disposal of Transitory Records

Employees are responsible for identifying transitory information and disposing of it when it is no longer needed.

Identification of Transitory Information

Government employees must distinguish transitory information from records and data that document decisions and actions.

- Transitory Information
  Transitory information is information of temporary usefulness that is not required to support or document a government body's actions and decision-making. Like other records, transitory information can exist in any format (paper or digital) and can be created and shared over a variety of media (e.g., email, social media, handwritten notes, voice mail, MS Teams, SharePoint, wikis, digital systems).

  Employees should dispose of transitory information, that does not fall under a current classification in ARCS or GPEB ORCS, with one important exception:
  - If a ministry 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 is subject to such requests must be retained pending completion of the applicable FOI response process and review period or the applicable litigation activities (contact GPEB.FOIManagement@gov.bc.ca).

  For assistance in determining whether information is transitory, refer to the:
  - Transitory Information Guide
  - Transitory Information Quick Tips
  - Managing Drafts and Working Materials Guide
  - Transitory Records Schedule (Schedule 102901).

- Documenting Government Decisions and Actions
  Government bodies have an obligation to create and keep adequate records to document their decision making and work activities. For assistance in determining which decisions and information must be retained, refer to:

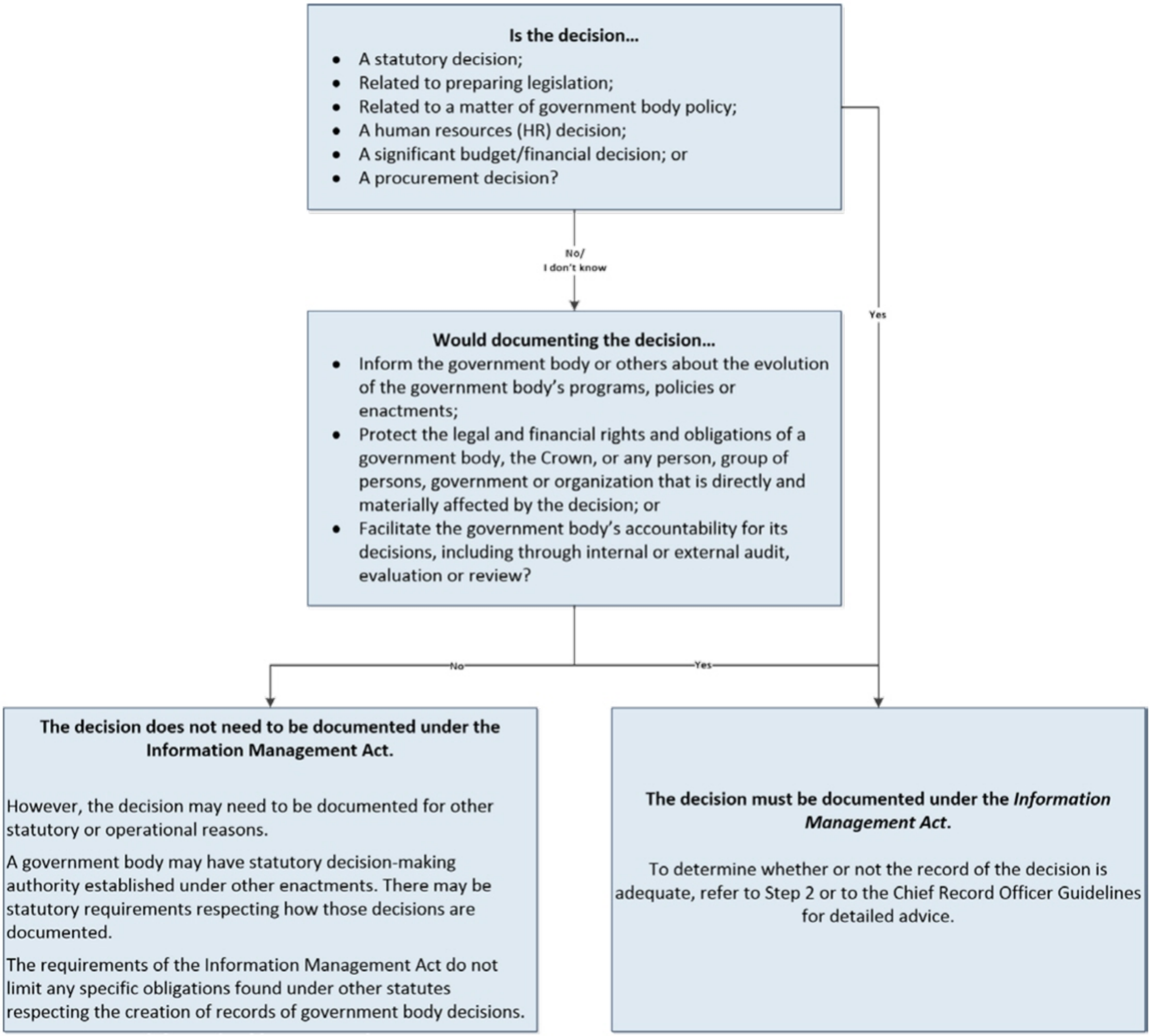
  - The flowcharts on the following pages.
  - CRO Guidelines on Documenting Decisions

  The requirement to document government decisions and actions also applies when those decisions are made via remote means such as online meetings.

  - See Online Meetings Guide

Identifying and Documenting Decisions

STEP 1: Does a Decision Need to Be Documented Under the *Information Management Act*?



Is the decision…

- A statutory decision;
- Related to preparing legislation;
- Related to a matter of government body policy;
- A human resources (HR) decision;
- A significant budget/financial decision; or
- A procurement decision?

Would documenting the decision…

- Inform the government body or others about the evolution of the government body's programs, policies or enactments;
- Protect the legal and financial rights and obligations of a government body, the Crown, or any person, group of persons, government or organization that is directly and materially affected by the decision; or
- Facilitate the government body's accountability for its decisions, including through internal or external audit, evaluation or review?

The decision does not need to be documented under the Information Management Act.

However, the decision may need to be documented for other statutory or operational reasons.

A government body may have statutory decision-making authority established under other enactments. There may be statutory requirements respecting how those decisions are documented.

The requirements of the Information Management Act do not limit any specific obligations found under other statutes respecting the creation of records of government body decisions.

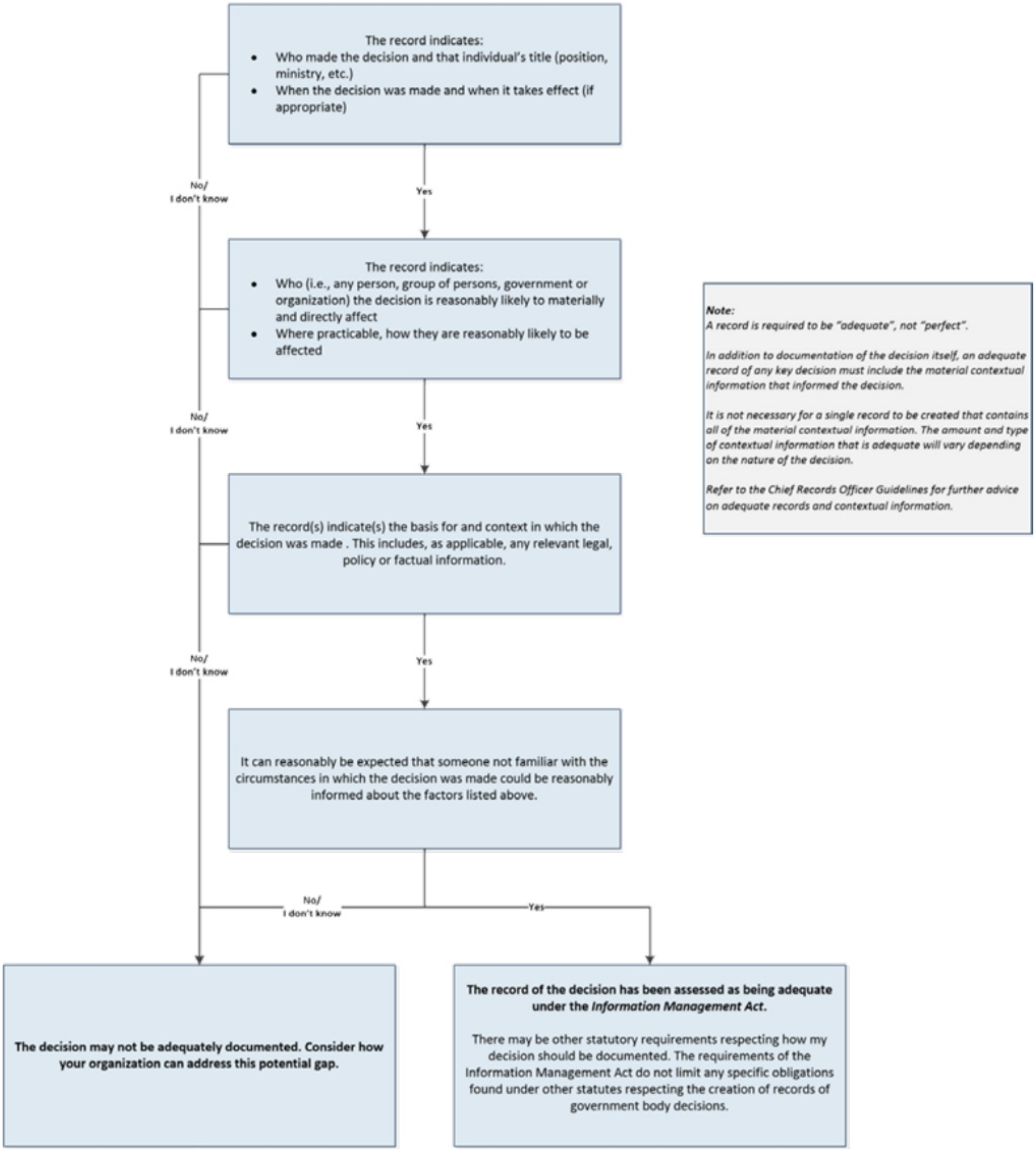
The decision must be documented under the *Information Management Act*.

To determine whether or not the record of the decision is adequate, refer to Step 2 or to the Chief Record Officer Guidelines for detailed advice.

SOURCE: *Chief Records Officer Guidelines on Documenting Government Decisions*, March 31, 2019

Identifying and Documenting Decisions

STEP 2: Is the Record of a Decision Adequate Under the *Information Management Act*?



The record indicates:

- Who made the decision and that individual's title (position, ministry, etc.)
- When the decision was made and when it takes effect (if appropriate)

The record indicates:

- Who (i.e., any person, group of persons, government or organization) the decision is reasonably likely to materially and directly affect
- Where practicable, how they are reasonably likely to be affected

The record(s) indicate(s) the basis for and context in which the decision was made . This includes, as applicable, any relevant legal, policy or factual information.

It can reasonably be expected that someone not familiar with the circumstances in which the decision was made could be reasonably informed about the factors listed above.

The decision may not be adequately documented. Consider how your organization can address this potential gap.

The record of the decision has been assessed as being adequate under the *Information Management Act*.

There may be other statutory requirements respecting how my decision should be documented. The requirements of the Information Management Act do not limit any specific obligations found under other statutes respecting the creation of records of government body decisions.

Note:
A record is required to be "adequate", not "perfect".

In addition to documentation of the decision itself, an adequate record of any key decision must include the material contextual information that informed the decision.

It is not necessary for a single record to be created that contains all of the material contextual information. The amount and type of contextual information that is adequate will vary depending on the nature of the decision.

Refer to the Chief Records Officer Guidelines for further advice on adequate records and contextual information.

SOURCE: *Chief Records Officer Guidelines on Documenting Government Decisions*, March 31, 2019

Disposal of Transitory Information

Routinely deleting transitory information ensures that the information being stored and managed by GPEB is the information it needs to keep. Employees do not need formal authorization to destroy transitory information unless:

1. The records do not fall under a current classification in ARCS or GPEB ORCS.
2. The records are needed for an FOI or legal search. Such records must be retained pending completion of the applicable FOI response process and review period or the applicable litigation activities.

Contact GPEB.RecordsManagement@gov.bc.ca for assistance with such records.

Employees must always ensure that destruction occurs in a secure manner.

- Government records and any records containing information about an individual should be placed into a locked bin in the office for appropriate disposal or destroyed using a cross-cut shredder.
- When working remotely, employees should use government issued devices to store and access work information rather than printing paper copies as this reduces the risk of unauthorized disclosure or loss.

2.6 Digitization of Records

GPEB is moving towards a fully electronic work environment. Consequently, any non-transitory records that are in physical format (e.g., paper) must be digitized via scanning prior to filing them in EDRMS or GOS (for operational records).

- See Scanning of Paper Records Policy

2.7 Redundant Records

Redundant Source Information (RSI) is government information that has been replaced and rendered redundant by authoritative copies once those copies have been verified to ensure their accuracy and authenticity. For example, after scanning a paper record, the scanned electronic version would be filed in the records repository and the paper copy would become a redundant record.

- Refer to 9C: Digitizing Records, Redundant and Transitory Records Schedule Processes for more information on redundant records.

Contact GPEB.RecordsManagement@gov.bc.ca prior to destroying any redundant records.

Related Policies

Click on the links below to view the following policies:

- Naming Conventions for Records and Folders
- Managing Government Emails
- Employee Notes
- Scanning of Paper Records

Section: **Records Management**	Issue Date: March 24, 2022
Subsection: DAY-TO-DAY RECORDS MANAGEMENT FOR GPEB EMPLOYEES	Revision Date:
	Page 1 of 3

Policy Name:

Naming Conventions for Folders and Records

Section 2, Section Title: 2.1 Naming of Records and Folders

Purpose*:*
This policy outlines the requirements for all GPEB staff when naming folders and records. The use of naming conventions will provide all staff with a common language to use when creating and searching for records.

Summary:
All GPEB folders and records created and/or saved in the Enterprise Document Records Management System Content Manager (EDRMS), Local Area Network (LAN), or collaboration tools, must adhere to the naming conventions as specified in this policy and outlined in the GPEB Records Master Matrix. This policy does not apply to records created and/or saved in the Gaming Online Service (GOS).

Relevant Section of Legislation or Regulation:

- Not applicable

Definitions:

"Collaboration tools" means applications or software that allow multiple users to work together on projects from any location and from different devices. Examples include, but are not limited to, MS Teams, Skype, SharePoint, eApprovals, OneDrive, and OneNote.

"Naming conventions" means agreed-upon standards for assigning record names.

"Records" means note logs/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, mechanic or otherwise.

"Record name" means a name used to uniquely identify a record.

Policy:

1.0 This policy applies to:

1.1 All records whether in draft or final form.

1.2 All folders and records created and/or saved in EDRMS, LAN, or collaboration tools.

2.0 This policy does not apply to:

2.1 Records created and/or saved in GOS.

3.0 Folder names and record names should adhere to the naming conventions outlined in the GPEB Branch Records Master Matrix.

3.1 If an appropriate naming convention cannot be found in the matrix, staff should contact GPEB.RecordsManagement@gov.bc.ca to request, with ED approval, the development of a new convention to be added to the GPEB Branch Records Master Matrix.

4.0 For folders, the naming conventions are:

4.1 Folder names should not exceed 75 characters.

4.2 An underscore should be used in between words. There should be a space on each side of the underscore.

4.3 All letters used in the folder names should be upper case (e.g., FOLDER _ NAME).

4.4 The use of acronyms in folder names should be avoided, if possible.

4.5 Date formats should be: YYYY or YYYYMM or YYYYMMDD

4.5.1 When referring to fiscal year, YYYY _ YYYY should be used.

4.6 Example of folder name: LEAN _ PROJECTS _ 2021

5.0 For records, the naming conventions are:

5.1 Record names should not exceed 100 characters.

5.2 An underscore should be used in between words. There should be a space on each side of the underscore.

5.3 The first letter of each word in the record name should be capitalized (e.g., Record _ Name).

5.4 Date formats should be: YYYY or YYYYMM or YYYYMMDD

6.4.1 When referring to fiscal year, YYYY _ YYYY should be used.

5.5 Example of record name: Lean _ Review _ PREG _ Internal _ Procedures _ 2021

6.0 Special characters (i.e., - ( ) { }[ ] * ^ % $ # & @ ! \ | : ' ; " ? /) should not be used in folder or record names unless the special character is part of a legal name. Example: AB&C Company Ltd. _ 2021

7.0 To reduce folder and record names to meet the character length requirements specified in this policy, staff should save important information in EDRMS using the notes field. When conducting a search in EDRMS, the search engine will check these fields.

Resources:

- Contact GPEB.RecordsManagement@gov.bc.ca for any questions or assistance with this policy.

Procedure:

- Procedure Module 4A: EDRMS – General Search Methods

Section: **Records Management**	Issue Date: March 24, 2022
Subsection: DAY-TO-DAY RECORDS MANAGEMENT FOR GPEB EMPLOYEES	Revision Date:
	Page 1 of 2

Policy Name:

Managing Government Emails

Section 2, Section Title: 2.3 Emails

Purpose*:*
This policy outlines the records management requirements for GPEB employees when managing emails.

Summary:
Emails pertaining to the business of government are considered to be government records and as such, all GPEB and government records management policies and legislative requirements apply. Key requirements of these acts and policies are outlined in this policy. All emails sent by GPEB staff, including replies, must contain the disclosure specified in this policy.

Relevant Section of Legislation or Regulation

- Not applicable

Policy:

1.0 Emails pertaining to the business of government are considered to be government records and as such, all records management and retention policies and legislative requirements apply. This includes, but is not limited to, the *Information Management Act* and schedules, and the *Freedom of Information and Protection of Privacy Act*.

2.0 GPEB employees are expected to follow the *Information Security Policy, Appropriate Use Policy* and Standards of Conduct for BC Public Service Employees when using or accessing government email. These requirements include, but are not limited to:

2.1 Employees must use a government email account when sending emails, including when working outside the office. Employees must not forward work emails or documents to their non-government email account.

2.2 Per section 2.2 of the *Appropriate Use Policy*, employees may use a government-issued IT device for reasonable personal use, as long as the use is limited during work hours, is lawful, does not compromise the security of government IT resources or government information, and is not used for personal financial gain.

3.0 GPEB employees should regularly delete transitory, superseded, and non-work information from their inboxes and folders. (See Email Guide below for more information about transitory emails.)

3.1 Emails should only be deleted or disposed of in accordance with approved information schedules.

3.2 Employees must never triple-delete emails (i.e., attempt to purge an email from their "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 the Outlook account.

4.0 GPEB employees are responsible for filing all emails that document government activities and decisions (i.e., non-transitory emails) in GPEB's records repository, the Enterprise Document Records Management System Content Manager (EDRMS) or Gaming Online Service (GOS) for emails relating to investigations (as per divisional procedures).

4.1 For emails received from sources within GPEB, it is the responsibility of the sender of the email to decide if the email and/or attachment(s) constitute an official record and if so, to file the email in EDRMS.

4.2 For emails received by GPEB employees from external sources, it is the responsibility of the principal receiver of the email to decide if the email and/or attachment(s) constitute an official record and if so, to file the email in EDRMS. The "principal receiver" is the sole recipient of an external email or, if there are several recipients, the recipient who is responsible for the most relevant work area.

4.3 For shared mailboxes, it is the responsibility of the person assigned responsibility for the mailbox to determine whether the email and/or attachment(s) constitute an official record and if so, to file the email in EDRMS.

5.0 All emails sent by GPEB staff, including replies, must contain the following disclosure:

*** CONFIDENTIALITY NOTICE***
This communication (both the message and any attachments) is intended for use by the person or persons to whom it is addressed and must not be shared or disseminated unless authorized by law or with the express authority of the sender. This communication may contain privileged or confidential information. If you have received this message in error or are not the named recipient, please immediately notify the sender and delete the message from your mailbox and trash without copying or disclosing it.

6.0 If a privacy breach occurs related to an email, employees and supervisors must follow the *Information Incident Management Policy*, which requires the immediate reporting of any suspected or actual information incident. (See Information Incidents.)

7.0 Employees should refer to the Email Guide (below) for further information and instruction for managing their government emails.

Resources:

- Contact GPEB.RecordsManagement@gov.bc.ca for any questions or assistance with this policy.
- Naming Conventions for Folders and Records Policy
- Email Guide

Procedure:

- See Procedure Module 5B: Moving Records in EDRMS

Section: **Records Management**	Issue Date: March 24, 2022
Subsection: DAY-TO-DAY RECORDS MANAGEMENT FOR GPEB EMPLOYEES	Revision Date:
	Page 1 of 2

Policy Name:

Employee Notes

Section 2, Section Title: 2.4 Employee Notes

Purpose*:*
This policy outlines the records management requirements relating to employee notes.

Summary:
Employee notes are government records. Employees are responsible for managing their notes in accordance with all records-related legislative and policy requirements. This includes filing all non-transitory employees notes in GOS (for notes relating to an Enforcement Division investigation) or EDRMS (for all other employee notes).

Relevant Section of Legislation or Regulation:

- Not applicable

Definitions:
"Employee notes" means work-related information, including images, recorded by an employee in the course of carrying out their duties. Employee notes may be recorded manually (e.g., in a physical notebook, notepad, calendar, appointment book, day timer or diary) or electronically (e.g., in OneNote, Word or other electronic application). Employee notes are government records and are subject to all policies relating to government records. Many employee notes are transitory in nature (e.g., action items).

Policy:

1.0 Employee notes must be managed in accordance with information schedules of the *Information Management Act* (i.e., ARCS, GPEB ORCS, and Special Schedules).

1.1 GPEB employees are responsible for filing all notes that document government activities and decisions (e.g., non-transitory employee notes) in a records repository.

1.1.1 Employee notes relating to an investigation are non-transitory and must be filed in either the Gaming Online Service (GOS) for notes relating to an investigation (as per divisional procedures) or EDRMS (for all other employee notes).

1.1.2 All other non-transitory employee notes must be filed in the Enterprise Document Records Management System Content Manager (EDRMS).

1.2 Once the employee notes have been transferred to EDRMS or GOS as applicable, the notebooks or pages containing the notes should be destroyed appropriately. (See *Disposal of Transitory Information*.)

2.0 When electronic notes are shared with other employees or team members, the primary owner of the notes is responsible for retaining and filing the notes. (See Use of Collaboration Tools Policy.)

Resources:

- Contact GPEB.RecordsManagement@gov.bc.ca for any questions or assistance with this policy.

- PLACEHOLDER: Link to Enf Div "Investigative Notebooks" policy

- RIM – Recorded Information Management Manual RIM 101 – Identifying Government Records RIM Pol 02-08 Administrative Amendment of Approved Records Schedules (gov.bc.ca)

- CRO Directive and Guidelines on Documenting Decisions: https://www2.gov.bc.ca/gov/content/governments/organizational-structure/ministries-organizations/central-government-agencies/corporate-information-records-management-office/information-management-act/cro-directives-guidelines

- Managing Drafts and Working Materials tip sheet: draftsworkingmaterials.pdf (gov.bc.ca)

Procedure:
Not applicable

Section: **Records Management**	Issue Date: March 24, 2022
Subsection: DAY-TO-DAY RECORDS MANAGEMENT FOR GPEB EMPLOYEES	Revision Date:
	Page 1 of 2

Policy Name:

Scanning of Paper Records

Section 2, Section Title: 2.3 Digitization of Records

Purpose*:*
This policy outlines the requirements relating to the digitization of GPEB's non-transitory paper records. The purpose of this policy is to enable GPEB to maintain an electronic work environment and to support electronic records management processes.

Summary:
GPEB program areas are required to scan all non-transitory paper records. The program area must consult with GPEB's FOI and Records Management for advice prior to scanning any paper records and/or destroying any records. The scanning must comply with the government's common standard for digitization.

Relevant Section of Legislation or Regulation:

- Sections 6, 10 and 11 of the *Information Management Act*

Policy:

1.0 All non-transitory paper records should be scanned.

1.1 Program areas must consult GPEB.RecordsManagement@gov.bc.ca prior to scanning any paper records.

1.2 Program areas are responsible for scanning applicable paper records.

2.0 The method and technology used to scan paper records must be in keeping with the Digitizing Government Information Standard.

3.0 Once a record that contains a wet signature has been scanned, the scanned record is deemed to be the original record.

4.0 A paper record that has been scanned may be destroyed once the scanned record is filed in the appropriate records repository.

4.1 When replacing original source information with copies, requirements established in the Redundant Source Information Guide must be met.

4.2 Program areas must consult GPEB's FOI and Records Management Unit (GPEB.RecordsManagement@gov.bc.ca) for advice prior to destroying any records.

Resources:

- Contact GPEB.RecordsManagement@gov.bc.ca for any questions or assistance with this policy.
- Digitizing Government Information Standard
- Redundant Source User Guide: https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/records-management/guides/rsruserguide.pdf

Procedure:

- Module 9C – Digitizing Records, Redundant and Transitory Records processes

3.0 Enterprise Document Records Management System Content Manager (EDRMS)

Purpose

1. Explain what EDRMS is.
2. Explain the access groups for EDRMS.
3. Provide links to EDRMS procedures.

3.1 About EDRMS

The Enterprise Document Records Management System Content Manager (EDRMS) is a records management system used by governments and the broader public sector worldwide to manage physical and electronic records throughout their life cycle. EDRMS ensures that records are captured, protected, retained, and destroyed in accordance with approved information schedules such as the Administrative Records Classification System (ARCS) and the Operational Records Classification System (ORCS). *(See Classification of Records for an explanation of the information schedules relevant to GPEB.)*

Through complete lifecycle management, EDRMS helps agencies:

- Ensure that all key activities and decisions are easily accessible and preserved for the requisite period of time;
- Reduce storage costs; and
- Enable timely search and retrieval of documents whenever they are required.

EDRMS is the records repository approved by the BC government and used by GPEB. With the exception of some operational records (e.g., investigation files), all GPEB records that require long-term retention must be filed in EDRMS.

The use of GOS rather than EDRMS as a records repository

Some GPEB divisions such as Licensing, Certification and Registration and Enforcement use Gaming Online Service (GOS), for primary intake from service providers or registrants, or throughout the investigative process. GOS is also the main work tool for investigators for some types of investigations, where it is utilized for retaining the investigation records for future reference or connections to other potential files or individuals.

GPEB employees will be required to store final versions of records in the appropriate EDRMS folders as soon as they are completed. Users who have opened the folders are required to close them according to the classification schedule. Please see Procedure Module 7 for procedures relating to the lifecycle of a folder.

In addition, GPEB employees have the option to maintain working documents in EDRMS or another collaboration platform. There are steps to take to overwrite the working version with the final version; the system will remove previous versions.

- See Use of Collaboration Tools Policy
- See Procedure Module 6B: Edit a Document in EDRMS

3.2 Access to Records in EDRMS

The level of access that an employee has to records in EDRMS depends on three things:

1. The employee's EDRMS user profile (sometimes referred to as their "role");
2. The access group the user has been assigned to; and
3. The permission assigned to the EDRMS folder in question.

Access groups and their associated permissions are determined by GPEB Executive. The approved list of access groups for the IGCO is listed in the Access Groups Policy. This list and the current list of access groups can also be found in the GPEB Records Master Matrix.

- Access Groups Policy
- Procedure Module 2A: Security – Permission and Restricted Access Overview

3.3 Media Files

All records received or created in the format of a media file must be filed in EDRMS, with the exception of some operational files which are filed in GOS (e.g., investigation-related media files), as explained above.

EDRMS media files cannot exceed 6MB in size. For media files larger than 6MB, employees should contact GPEB.RecordsManagement@gov.bc.ca

JPEG is the preferred file type for media records filed in EDRMS. Other acceptable file types include:

- Adobe Illustrator (.ai)
- Adobe Photoshop (.psd)
- AVI (.avi)
- Encapsulated Postscript (.eps, .epsf, or .epsi)
- MP3 (.mp3)
- MPEG (.mpg)
- WAVE Audio (.wav or .wave)
- Windows Media (.wmv)

In order for a media file to be opened in EDRMS, program areas should ensure that employees have the appropriate software on their computers. If software for the required file type is not listed above, contact GPEB.RecordsManagement@gov.bc.ca for assistance.

- See [link to media files procedure]

3.4 EDRMS Procedures

Click on the links below for instructions on how to use EDRMS:

MODULE #	TOPIC	PROCEDURE
2A	Access & Security	Security – Permission and Restricted Access Overview
2B	Access & Security	File Creator Questionnaire Checklist
3A	Configuration	EDRMS Basic Configuration
3B	Configuration	EDRMS Configurating Display Options
3C	Configuration	Downloading EDRMS Software
4A	Searching	EDRMS – General Search Methods
4B	Searching	EDRMS – Advanced Search Features (Document Content, Complex, Refine, Wildcard, Misc.)
4C	Searching	EDRMS – Advanced Search Features (Boolean Searches, String Based Searches)
4D	Searching	EDRMS – Searching Features and Functions
5A	Folders	Create Folder in EDRMS
5B	Folders	Moving Records in EDRMS
5C	Folders	Create Folder in EDRMS – Template
5D	Folders	Relating or Cross Referencing Folders in EDRMS
5E	Folders	EDRMS Folders – Create Parts
5F	Folders	Create Folder References in EDRMS
5G	Folders	Information Aid – Create a Folder in EDRMS
6A	Documents	Create a Document in EDRMS
6B	Documents	Edit a Document in EDRMS
8A	Emails	Moving Email Records to EDRMS
8B	Emails	Managing Email Checklist

Related Policies

Click on the links below to view the following policies:

- Access Groups for EDRMS

Section: **Records Management**	Issue Date: March 24, 2022
Subsection: EDRMS	Revision Date:
	Page 1 of 2

Policy Name:

Access Groups for EDRMS

Section 3, Section Title: 3.2 Access to Records in EDRMS

Purpose*:*
This policy outlines the requirements relating to the access groups for GPEB in the Enterprise Document Records Management System Content Manager (EDRMS).

Summary:
The approved GPEB access groups for EDRMS are listed in this policy. Any changes to these access groups must be approved by GPEB Executive.

Relevant Section of Legislation:

- Section 19 of the *Information Management Act* (This section is further defined by section 1.11 of the Appropriate Use Policy, and section 1.5 of the Managing Government Information Policy.)

Policy:
Access groups are created in EDRMS to ensure that records can only be accessed by those employees with permission to access them. Each access group is typically comprised of employees that belong to a common program area and/or initiative. Access groups/permissions are applied to folders at the time of their creation in EDRMS.

1.0 This policy only applies to records in EDRMS.

2.0 The approved GPEB access groups for EDRMS are listed in the following table.

2.1 Any changes to these access groups must be approved by GPEB Executive.

IGCO ACCESS GROUPS (FUTURE)		
GPEB Division or Group	***New Access Group Name**	**New Access Group Members**
GPEB DIVISIONS		
Assistant Deputy Minister's Office	ADMO	ADM; Executive Coordinator; Executive Assistant; ADMO staff
Licensing Registration, and Certification	Licensing, Registration and Certification	Licensing, Certification and Gaming Integrity; Personnel and Lottery Retailer Registration
	Corporate Registration	Corporate Registration
Operations	Operations	Information and Technology; Finance and Facilities; Freedom of Information and Records Management
	Workforce Planning/HR	Workforce Planning/HR staff
Compliance	Audit	Commercial; Charitable
	Horse Racing	Stewards; Judges; Horse racing staff
Enforcement	Investigations	Investigation staff
	Intelligence	Intelligence staff
Strategic Policy and Projects Division	SPPD	SPPD staff
Community Supports Division	Gambling Support BC	CSD staff
MISCELLANEOUS GROUPS		
Executive	Executive (Group)	
	Directors	
	Managers	
	Leads	
	Projects (*on an as needed basis)	
INDIVIDUAL EXECUTIVE DIRECTORS		
*(*related to Workforce Planning only)*		
	Alistair Cochrane	
	Anna Fitzgerald	
	Cary Skrine	
	David Horricks	
	David Nicholson	
	Jillian Hazel	
	My Anh Truong	
	Steve Pleva	
ADMINISTRATIVE RECORDS GROUPS		
Record Key Holders (Jamie, Cathy, Sylvia) Administrative Records Support (Program area administrative staff)		

3.0 Records belonging to the following program areas are restricted to employees belonging to the access group as listed in the table above.

- Workforce Planning

- Investigations
- Intelligence
- Assistant Deputy Minister Office
- Corporate Registration

4.0 If an employee accesses a record, they should not have access to they must contact GPEB.RecordsManagement@gov.bc.ca

Resources:

- Contact GPEB.RecordsManagement@gov.bc.ca for any questions or assistance with this policy.
- GPEB Records Master Matrix

Procedure:

- Procedure Module 2A: Security – Permission and Restricted Access Overview
- Procedure Module 5A: Create Folder in EDRMS

4.0 Applications and Systems Used in the Day-to-Day Management of GPEB Records

Purpose

1. Provide an overview of the storage points commonly used by GPEB employees when managing records in active use.
2. Explain the requirements for employees to manage their H: Drives.
3. Outline the process for employees to obtain permission to use applications or software that has not been pre-approved by GPEB.

4.1 Storage Points for Active GPEB Records

Table 2, below, lists the applications, systems and devices commonly used by GPEB employees while records are in active use. This is not an exhaustive list.

The applications, systems and devices listed in Table 2 should be viewed as "working environments" for records. At a certain point in the records life cycle – usually once the records are no longer being actively used - all non-transitory records in these applications and systems must be filed in EDRMS, with the exception of some operational records (e.g., investigation files) which are filed in the Gaming Online Service (GOS).

Table 2: Records Storage Points

APPLICATION/ SYSTEM	DESCRIPTION	RELATED POLICY OR SECTION
CLIFF	A corporate correspondence tracking system used by Ministry offices to track high volumes of executive correspondence. CLIFF is not a record keeping system; all documents must be filed in EDRMS.	Corporate Approval Tools Policy
Collaboration tools	Applications or software that allow multiple users to work together on projects from any location and from different devices. Examples include, but are not limited to, MS Teams, Skype, SharePoint, eApprovals, OneDrive, and OneNote.	Use of Collaboration Tools Policy
eApprovals	A SharePoint site created to guide documents through GPEB and/or Ministry executive for signoff. It is a short-term collaboration tool; once signed, the documents must be filed in EDRMS.	Corporate Approval Tools Policy
EDRMS	A records management system used by GPEB to manage physical and electronic records throughout their life cycle.	Enterprise Document Records Management System Content Manager (EDRMS)

APPLICATION/ SYSTEM	DESCRIPTION	RELATED POLICY OR SECTION
	With the exception of some operational records (e.g., investigation files), all GPEB records that require long-term retention must be filed in EDRMS.	
External storage devices	Mobile media that is used to transfer and/or store electronic records. This includes, but is not limited to, magnetic, optical, flash memory, and recording devices. This does not include mobile phones or laptops.	External Storage Devices Policy
Gaming Online Service (GOS)	An internal-facing application used by GPEB staff to process applications and manage registration-related records, including investigation reports and decisions. GOS is also an external-facing, web-based application used by applicants to submit applications and pay application fees for gaming worker registration. Some operational records (e.g., investigation files) are filed in GOS, not EDRMS.	Use of GOS rather than EDRMS as a records repository
H: Drives	An employee's personal drive. It is accessible to the employee only and should not contain government records.	Managing H: Drives
Local Area Network (LAN)	A computer network that interconnects computers within a limited area such as government. GPEB employees are responsible for ensuring all non-transitory records created in the LAN are filed in GPEB's records repository (i.e., EDRMS or GOS).	Not applicable

For more information about the appropriate systems to use for managing records, see the *Appropriate Recordkeeping System Records Management Guide*

4.2 Managing H: Drives

An H: Drive is an employee's personal drive. It is accessible to the employee only and should only be used to store things that only the employee requires access to (e.g. MyPerformance planning materials, requests related to time and leave, course materials, resumé).

To protect personal privacy, and to reduce government's digital storage costs, employees must limit the amount of information that they store on government networks for personal reasons (e.g., family photos, personal documents). Per government guidelines, information stored on the H: Drive should not exceed a 100 MB storage limit. Government records should always be stored in the appropriate repository (i.e., GOS for some operational records such as investigation files, or EDRMS for all other GPEB records.).

- See personal_storage_H_drive_quick_tips.pdf (gov.bc.ca)

4.3 Obtaining Permission to Use Other Applications or Software

To prevent concerns relating to issues such as information security and costs, all software and applications used by GPEB employees must be approved for use.

All applications, systems and devices listed in Table 2, above, have been approved for use by GPEB employees. If an employee wishes to download an application or software that is not listed on the table above, they must do the following, in keeping with section 3 of the OCIO's Appropriate Use Policy:

- Determine if the application or software is available via a BC Government–supplied App Store (e.g., OCIO My Service Centre) and contact GPEB.LOB@gov.bc.ca for further assistance.
- If the application or software is not available via one of these sources, the employee must first obtain their supervisor's permission before accessing or downloading the application or software.
- Supervisors must not permit an employee to download or use applications or software that:
    - are prohibited by the Office of the Chief Information Officer;
    - present unacceptable privacy or security risks;
    - impose terms and conditions, such as indemnification clauses, that are unacceptable to government (see CPPM Chapter 6).

Supervisors should refer to the Application and Software Guide to assist them in assessing the appropriateness of any software requested by employees.

For questions about specific applications or software, please contact GPEB.LOB@gov.bc.ca
GPEB IT/LOB Support can assist all employees in the interpretation and application of this policy, as well as act as a conduit for supervisors to the Ministry Information Security Officer.

Related Policies

Click on the links below to view the following policies:

- Corporate Approval Tools
- Use of Collaboration Tools
- External Storage Devices

Section: **Records Management**	Issue Date: March 24, 2022
Subsection: APPLICATIONS AND SYSTEMS USED IN THE DAY-TO-DAY MANAGEMENT OF GPEB RECORDS	Revision Date:
	Page 1 of 3

Policy Name:

Corporate Approval Tools

Section 4, Section Title: 4.1 Storage Points for Active GPEB Records

Purpose*:*
This policy outlines the records management requirements for obtaining executive-level approvals for GPEB documents.

Summary:
All GPEB correspondence and briefing notes should be logged in CLIFF; any document requiring approval should be entered into eApprovals. All documents requiring ADM approval or above must be routed per Appendix A (below).

Relevant Section of Legislation or Regulation:

- Not applicable

Definitions:

"CLIFF" is a corporate correspondence tracking system used by Ministry offices to track high volumes of executive correspondence. CLIFF is not a records repository; all executive correspondence must be filed in the Enterprise Documents Records Management System Content Manager (EDRMS).

"eApprovals" is a SharePoint site created to guide documents through GPEB and/or Ministry executive for signoff. It is a short-term collaboration tool, not a records repository. Once signed, the documents must be filed in EDRMS.

Policy:

1.0 All GPEB correspondence and briefing notes should be entered into CLIFF for government tracking purposes.

1.1 Divisional Administrative Assistants are responsible for creating CLIFF logs.

2.0 Any document that requires approval at the Executive Director level or above including Assistant Deputy Minister, Associate Deputy Minister, Deputy Minister or Minister should be entered into eApprovals.

3.0 The Executive Director of the program area that drafted the document(s) is responsible for ensuring the appropriate approvals are obtained prior to the document being sent to the Assistant Deputy Minister for approval.

3.1 If more than one program area is involved in drafting the document(s), both Executive Directors need to approve the document(s).

4.0 All GPEB documents requiring approval from the Assistant Deputy Minister, Deputy Minister or Minister should be routed as described in Appendix A (attached).

5.0 Cliff logs and eApprovals should be closed in accordance with Ministry procedures, and the eApproval printable history report and the approved and document with signature filed with the corresponding document in EDRMS.

Resources:

- Contact GPEB.RecordsManagement@gov.bc.ca for any questions or assistance with this policy.
- Cliff User Guide:
  cliff_6_user_guide_v01_3.pdf (gov.bc.ca)
- Ministry Correspondence Guide:
  PSSG Correspondence Guide - Publications - Attorney General and Public Safety and Solicitor General (gov.bc.ca)

Procedure:

- Not applicable

APPENDIX A: GPEB eApproval Routing

Acronyms

ADM – Assistant Deputy Minister	**EC –** Executive Coordinator
CCU – Corporate Correspondence Unit	**ED –** Executive Director
DM – Deputy Minister	**PA** – Program Area
EAA – Executive Administrative Assistant	**CO** – GPEB Communications Officer

Document Type	**eApproval Routing (by Position Titles)**
Information or Decision Briefing Notes	
Information Briefing Note for ADM	PA-ED-EC-ADM-EAA
Decision Briefing Note for ADM	PA-PA ED-ED SPPD-EC-ADM-EAA
Information or Decision Briefing Note for DM	PA-PA ED-ED SPPD-EC-ADM-EAA-DM
Information or Decision Briefing Note for Minister	PA-PA ED-ED SPPD-EC-ADM-EAA-DM-Minister
*Documents will be returned to PA admin for filing in EDRMS once final approval has been obtained	
Travel/Training/Business Expense Approval Requests	
In province travel request	PA-Director-ED
Conferences (virtual and in-province)	PA-Director-ED-EC-ADM-EAA
Out of province travel or conferences	PA-Director-ED-ED-EC-ADM-EAA-DM
Business Expense Approvals	PA-Director ED-EC-ADM-EAA
*Documents will be returned to PA admin for filing in EDRMS once final approval has been obtained	
Correspondence	
Ministerial correspondence	ED-ED Policy-EC-ADM-EAA-CCU-DM-Minister
ADM correspondence (for ADM signature)	ED-EC-ADM-EAA-SPPD-CO
Branch-generated correspondence	ED-EC-ADM-EAA-SPPD-CO

Section: **Records Management**	Issue Date: March 24, 2022
Subsection: APPLICATIONS AND SYSTEMS USED IN THE DAY-TO-DAY MANAGEMENT OF GPEB RECORDS	Revision Date:
	Page 1 of 2

Policy Name:

Use of Collaboration Tools

Section 4, Section Title: 4.1 Storage Points for Active GPEB Records

Purpose:
This policy outlines the requirements for GPEB staff when managing records created, received and/or stored in collaboration tools such as MS Teams, Skype, SharePoint, eApprovals, OneDrive, and OneNote.

Summary:
GPEB employees must submit requests to GPEB.LOB@gov.bc.ca to create a team in MS Teams or a site in SharePoint. All policies relating to GPEB records also apply to records in collaboration tools. All non-transitory records, including any decisions made in collaboration tools and chat messages, must be filed in the Enterprise Document Records Management System Content Manager (EDRMS).

Relevant Section of Legislation or Regulation:

- Section 19 (1.1) of the *Information Management Act*
- CRO Directive 01-2019

Definitions:

"Collaboration tools" means applications or software that allow multiple users to work together on projects from any location and from different devices. Examples include, but are not limited to, MS Teams, Skype, SharePoint, eApprovals, OneDrive, and OneNote.

"Chat message" means a message created using the synchronous message functionality of a collaboration tool. Chat messages allow two or more people to communicate in real time.

Policy:

1.0 All policies relating to GPEB records also apply to all records created, received and/or stored in collaboration tools. This includes, but is not limited to, policies or guidelines relating to naming conventions, acronyms, transitory records, and the use of approved software.

2.0 GPEB employees must submit requests to GPEB.LOB@gov.bc.ca to do the following:

2.1 Create a team in MS Teams.

2.2 Create a site in SharePoint.

3.0 A collaboration tool is not a records repository. Employees are responsible for ensuring all non-transitory records created, received and/or stored in collaboration tools are filed in a records repository, EDRMS or GOS, as applicable.

3.1 When multiple individuals are utilizing a collaboration tool for a joint purpose, a "primary owner" must be assigned at the start of the initiative. The primary owner is responsible for ensuring the records in the collaboration tool are properly managed and filed.

4.0 Pursuant to section 19(1.1) of the *Information Management Act* and any related order(s), any information within collaboration tools that provides evidence of a decision must be documented and filed in a records repository, EDRMS or GOS.

4.1 Any decision(s) contained in a chat message should be copied, summarized, or transcribed to a Word document and filed in EDRMS as soon as practicable after the chat has concluded, as some collaboration tools automatically delete chat messages after a certain period of time.

4.2 If a collaboration tool is being used for inter-ministry or inter-jurisdictional purposes, a lead ministry should be identified as responsible for the committee's records at the start of the initiative. Each participating ministry/agency is responsible for records management of the shared files (e.g., documentation of decisions).

Resources:

- Contact GPEB.RecordsManagement@gov.bc.ca for any questions or assistance with this policy.
- Records management guides for MS Teams, SharePoint and OneNote:
  Collaboration Tools RM Guide (gov.bc.ca)
- CRO Directive and Guidelines on Documenting Decisions:
  https://www2.gov.bc.ca/gov/content/governments/organizational-structure/ministries-organizations/central-government-agencies/corporate-information-records-management-office/information-management-act/cro-directives-guidelines
- Information Management in the Cloud (gov.bc.ca)

Procedure:

- Not applicable

Section: **Records Management**	Issue Date: March 24, 2022
Subsection: APPLICATIONS AND SYSTEMS USED IN THE DAY-TO-DAY MANAGEMENT OF GPEB RECORDS	Revision Date:
	Page 1 of 2

Policy Name:

External Storage Devices

Section 4, Section Title: 4.1 Storage Points for Active GPEB Records

Purpose*:*
This policy outlines the records management requirements for GPEB staff when using external storage devices.

Summary:
Employees should only use external storage devices as a last resort, when all other means of records transfer have been exhausted. When such a device is used, employees must ensure that the records are encrypted and transferred to the records repository as soon as practicable.

Relevant Section of Legislation or Regulation:

- Not applicable

Definitions:
"External storage devices" means mobile media that is used to transfer and/or store electronic records. This includes, but is not limited to, magnetic, optical, flash memory, and recording devices. This does not include mobile phones or laptops.

Policy:

1.0 As the use of external storage devices increases the risk of records becoming compromised due to loss, theft or damage, such devices should only be used as a temporary solution or last resort, when all other means of records transfer have been exhausted. Whenever possible, other more secure means of records transfer should be used.

2.0 Per the Office of the Chief Information Officer's *Asset Management Security Standard*, if an external storage device is used to transfer or store records:

2.1 The records on the device must be encrypted. If GPEB staff are not sure if the external storage device meets the encryption requirements of this policy, they should contact GPEB.LOB@gov.bc.ca or GPEB.RecordsManagement@gov.bc.ca

2.2 The device must never be used to store the only version of a record; the records should be transferred as soon as practicable from the external storage device to either GOS (for some operational records such as investigation files) or EDRMS (for all other GPEB records).

3.0 If a privacy breach occurs in relation to a lost or stolen external storage device, employees and supervisors must follow the *Information Incident Management Policy*, which requires the immediate reporting of any suspected or actual records incident. (See Information Incidents.)

Resources:

- Contact GPEB.RecordsManagement@gov.bc.ca for any questions or assistance with this policy.
- Asset Management Security Standard https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/623_asset_management_security_guidelines_v10_-_final.pdf
- Cryptographic Standards for Information Protection https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/cryptographic_standards.pdf
- https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/resources/directions/encryption-personal-information-memorandum.pdf

Procedure:

- Not applicable

5.0 Handling of Personal and Confidential Information

Purpose

1. Outline the process for employees to follow in the event of a breach of private or confidential information.
2. Explain Privacy Impact Assessments and Information Sharing Agreements and employee responsibilities with respect to those agreements.

Definitions

- **Confidential information** includes Cabinet confidences, government economic or financial information, information harmful to intergovernmental relations, and third-party business information, where the disclosure of the information would harm the third party.
- **Information security** is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
- **Personal information** is recorded information about an identifiable individual other than business contact information; it includes such things as age, gender, and marital status. The *Freedom of Information and Protection of Privacy Act* (FOIPPA) sets out requirements pertaining to the collection, use and disclosure of personal information by public sector bodies.

5.1 Collection and Use of Personal Information

Privacy Impact Assessments

- A privacy impact assessment (PIA) is a step-by-step review process to determine whether a project involves the collection of personal information and if so, to ensure:
    - the information proposed to be collected is authorized under an Act; and
    - the protection of any personal information collected or used in the project.

  Completing a PIA is a legislative requirement, pursuant to section 69 (5.1) of FOIPPA.
- A PIA must be completed whenever an enactment, system, project, program, or activity is developed or amended. A PIA must be completed even if it is determined there is no personal information being collected, used, or disclosed. In cases where a program wants to collect additional personal information or use the information in way that is different than stated in the original PIA, a new PIA is required to be developed.
- Program area staff are responsible for drafting PIAs, while GPEB records management staff are responsible for assisting the program areas in drafting PIAs and for filing the PIAs in GPEB's recordkeeping system.

When a Privacy Impact Assessment is Required:

- GPEB program areas should contact GPEB.RecordsManagement@gov.bc.ca to begin the process of drafting a PIA.
- The steps for completing a PIA, as well as the applicable templates, are outlined at: https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments

Information Sharing Agreement

- An Information Sharing Agreement (ISA) is an agreement between a public body and another public body, person or group of persons, prescribed entity or organization that sets the conditions on the collection, use or disclosure of personal information by the parties to the agreement. Completing an ISA is a legislative requirement, pursuant to section 69 of FOIPPA.
- An ISA is required when a data-linking initiative or integrated program is proposed that will share personal information collected by GPEB with another public body or organization. An ISA is also required where another public body or organization proposes to share its personal information with GPEB.
- Program area staff are responsible for drafting ISAs, while GPEB records management staff are responsible for assisting the program areas in drafting ISAs and for filing the ISAs in GPEB's recordkeeping system.
- An ISA may require review and advice by Legal Services Branch (LSB) and is the divisional Executive Director's responsibility to ensure an ISA receives the appropriate LSB review.

To determine if an Information Sharing Agreement is required:

- The program area should contact GPEB.RecordsManagement@gov.bc.ca and refer to the Information Sharing Agreement Guidance, prepared by the Corporate Information and Records Management Office.

To prepare an Information Sharing Agreement:

- GPEB staff should use the ISA Template when preparing ISAs.
- The minister's order outlining the requirements for completing an ISA can be found here: Information-Sharing Agreement Directions (ISA Directions).

5.2 Information Incidents (i.e., Breaches of Privacy or Confidentiality)

Information incidents occur when unwanted or unexpected events threaten privacy or information security. A privacy breach is a type of information incident that involves personal information about people, such as names, birthdates, social insurance numbers or client information. Breaches may similarly occur with respect to confidential information.

Information incidents can be accidental or deliberate and include the theft, loss, alteration, or destruction of information. Examples include:

- ○ Loss of a computer, laptop, mobile device, or memory media such as flash drive and external hard drive that contains personal or confidential information.

- Sending an email or fax containing personal or confidential information to an unintended party.
- Placing a document containing personal or confidential information in a public recycling bin, rather than shredding it.
- Mailing or couriering material containing personal or confidential information to the wrong party or address.
- Exposure or provision of a password to an individual who is not authorized to use the password.

For privacy breaches and other information incidents, it is important to take immediate action.

If an information incident occurs, employees and supervisors must follow the *Information Incident Management Policy*, which requires the immediate reporting of any suspected or actual information incident (including a privacy breach or cyber-attack/phishing).[2]

In the event of an actual or suspected information incident - including a privacy breach - GPEB employees must[3]:

1. Report the incident immediately* to:
   a. their supervisor;
   b. their Executive Director;
   c. GPEB.RecordsManagement@gov.bc.ca as GPEB's FOI and Records Unit is responsible for tracking and storing this information in EDRMS and ensuring all the steps have been completed; and
   d. the Office of the Chief Information Officer (OCIO) by calling 250-387-7000 or toll-free 1-866-660-0811.

   **The requirement for immediate reporting applies at all times (24x7, 365 days a year), including after-hours, weekends and holidays.*

2. Take steps to contain the information incident, including recovering the information, wherever possible. This can include asking that information be returned or destroyed, suspending the activity that led to the incident or correcting the physical weakness that led to the incident. For example, if the incident involved sending an email to an unintended party, the employee must send another email to the recipient, advising them to delete the first email from their inbox and to reply back/advise when the email has been deleted.

3. If a General Incident or Loss Reporting Form is required, complete a General Incident or Loss Reporting Form, in accordance with Procedure L3 of the *Core Policy and Procedures Manual*: https://gilr.gov.bc.ca/within 24 hours.

[2] Employees learn about this reporting requirement and process in the mandatory IM117 information management course: Records Management Guides and Learning - Province of British Columbia (gov.bc.ca)

[3] Pursuant to Section 12.3.6(b)(2) of the *Core Policy and Procedures Manual*

4. Follow the remaining steps outlined in the Information Incident Checklist. *The specific responsibilities of ministry employees, supervisors, service providers and the Ministry Chief Information Officer are outlined in the Information Incident Management Policy.*

Related Policies

Click on the links below to view the following policies:

- External Storage Devices

6.0 Freedom of Information Requests

Purpose

Explain what a Freedom of Information (FOI) request is, and GPEB employees' role in the FOI process.

6.1 About FOI Requests

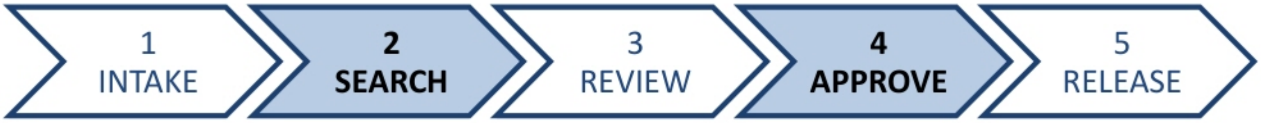
The *Freedom of Information and Protection of Privacy Act* (FOIPPA) establishes an individual's right to request and obtain records in the custody or control of a public body (including access to one's own personal information) when those records are not routinely available. Requests for information made under FOIPPA are referred to as FOI requests. Anyone can make an FOI request including individuals, political parties, the media and law firms, businesses, researchers, interest groups, and other governments.

FOIPPA requires public bodies such as GPEB to make every reasonable effort to assist applicants and to respond openly, accurately, completely and without delay to FOI requests. The principle behind the FOI process is that information should be released unless there is a good reason not to release. The public's right to access records is subject to limited exceptions to disclosure; information excepted from disclosure is removed from records released through FOI, with the exceptions noted.

The Information Access Operations division (IAO) of the Corporate Information and Records Management Office (CIRMO) has a lead role in ensuring government meets its legislated responsibilities with regard to FOI requests.

6.2 GPEB's Role in the FOI Process

The graphic below illustrates the five steps in an FOI request process. Steps 2 and 4 (in blue) are the steps that involve GPEB staff.



1. Intake

IAO receives all FOI requests and assists applicants in refining their requests so that they meet legislated requirements and are as clearly defined and specific as possible. IAO then forwards a Call for Records (CFR) form to the appropriate Ministry, which in turn sends it to the relevant Branch.

2. Search

When GPEB's FOI staff receive a CFR, they forward it to the appropriate program area to conduct a comprehensive records search. Pursuant to section 6(1) of FOIPPA, public servants have a duty to assist applicants and must make every reasonable effort to respond to every FOI request openly, accurately, completely and without delay. For GPEB employees, this includes:

- Interpreting FOI requests in good faith as a fair and rational person would expect. This means making a solid effort to discern the intent and goal of the applicant and steering clear of overly narrow interpretations.
- Searching all potential sources for records including, but not limited to:
    - Hardcopy files
    - GOS
    - CLIFF
    - EDRMS
    - Offsite records
    - LAN
    - Collaboration tools (e.g., SharePoint, TEAMS)
    - Databases
    - Email accounts (all folders including 'deleted' and 'sent'
    - Outlook calendars
    - Texts and instant messages (Skype/phone)
    - Staff notebooks
- Treating the request as urgent and conducting the searches as quickly as possible. Section 7(1) of FOIPPA requires that the government respond not later than 30 days after receiving the FOI request.

3. Review

IAO reviews and analyzes the information received from GPEB line-by-line and redacts it, where necessary, based on FOIPPA requirements. This is to ensure that the information is legally appropriate for release to the person who has asked for it.

4. Approve

IAO sends a copy of the reviewed material to the Ministry/GPEB for approval by the program area Executive Director and the Assistant Deputy Minister.

5. Release

IAO releases the records package to the applicant and publishes it to the Open Information website, where applicable.

If a ministry 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 is subject to such requests must be retained pending completion of the applicable FOI response process and review period or the applicable litigation activities. For more information, contact GPEB.FOIManagement@gov.bc.ca

Contact GPEB.FOIManagement@gov.bc.ca for assistance with any questions about FOI requests or process.

7.0 Departing Employees

Purpose

Explain the records management-related processes and requirements that must be followed when employees leave GPEB.

7.1 Departing Employees

All GPEB employees who are leaving the BC Public Service or transferring to a different branch or ministry within the BC Public Service must take steps, along with the supervisor, to ensure their records are in order prior to their departure.

These requirements apply to all employees, whether the leave is planned or unplanned.

Related Policies

Click on the links below to view the following policies:

- Records Management for Departing Employees

Section: **Records Management**	Issue Date: March 24, 2022
Subsection: DEPARTING EMPLOYEES	Revision Date: Page 1 of 3

Policy Name:

Records Management for Departing Employees

Section 7, Section Title: 7.1 Departing Employees

Purpose*:*
This policy outlines the records management requirements for GPEB employees who are leaving the BC Public Service (BCPS) or transferring from GPEB to another position within the BCPS.

Summary:
When an employee is departing GPEB, the employee's supervisor must alert GPEB's Records Management staff as soon as they become aware the employee will be leaving GPEB or prior to the employee's IDIR becoming inactive. Both the employee and the supervisor have specific responsibilities (as outlined in this policy) that vary depending on whether the leave is planned or unplanned. In all cases, a Secure Records Form must be completed.

Relevant Section of Legislation or Regulation:

- Not applicable

Definitions:

"Departing employee" means a GPEB employee who is leaving the BCPS or transferring to a different branch or ministry within the BCPS.

"Planned leave" includes temporary appointment in a different branch or ministry, retirement, resignation or other planned leave where an employee's IDIR will be transferred out of GPEB or become inactive.

"Records" includes both physical and digital records.

"Transitory records" means records of temporary usefulness that are needed only for a limited period of time in order to complete a routine action or prepare a final record. Transitory records are not required for financial, legal, audit or statutory purposes and are not filed in the records repository.

"Unplanned leave" includes termination, extended leave, or other unplanned leave where an employee's IDIR will be transferred out of GPEB or become inactive.

Policy:

1.0 The departing employee's supervisor must alert GPEB.RecordsManagement@gov.bc.ca as soon as they become aware the employee will be leaving GPEB or prior to an employee's IDIR becoming inactive, to ensure that proper steps are taken prior to the employee's departure. (See Procedures, below.)

2.0 The Secure Records Form (below) must be completed each time an employee departs GPEB.

2.1 In cases of unplanned leave, the departing employee's supervisor or Executive Director is responsible for notifying the GPEB Records Team Lead prior to the employee's IDIR becoming inactive in order to secure records.

2.2 In cases of planned leave, the GPEB FOI and Records Team Lead is responsible for meeting with employees to go over the Secure Record Form prior to their departure.

2.3 In cases of planned leave, the departing employee's supervisor or Executive Director is responsible for confirming the employee has completed the action items noted on Secure Record Form.

3.0 In cases of planned leave, departing employees are responsible for:

3.1 Cleaning out all personal storage (e.g., personal drives, email accounts).

3.2 Destroying or deleting all transitory records.

3.3 Returning any physical folders, external storage devices and/or recording devices to their supervisor. In situations where records are temporarily on an external storage device, the departing employee is responsible for ensuring their supervisor can access the device content.

3.4 Ensuring all records are filed in the appropriate records repository (i.e., the Electronic Documents Records Management System or the Gaming Online Service).

4.0 Departing employees must not take any confidential government records or records relating to GPEB business with them when they leave the BC Public Service or transfer to another position within the BC Public Service.

5.0 Departing employees may only take copies of non-confidential government records (e.g., work samples) if their Executive Director approves the action. Decisions of this nature must be made in consultation with the GPEB Records Unit and in certain circumstances the Ministry Privacy Officer.

Resources:

- Contact GPEB.RecordsManagement@gov.bc.ca for any questions or assistance with this policy.
- Template for GPEB Secure Records Review
- *Departing or Transferring Employees Guide*

Procedure:

- Offboarding | Gaming Policy and Enforcement Branch Intranet (gov.bc.ca)

8.0 Procedures

Purpose

1. Provide links to all GPEB records management and EDRMS procedure modules.

Records Management Overview and Classifications:

1A: Records Management Overview
1B: Records Management Classification Systems

EDRMS – Access Security and Permissions:

2A: Security – Permission and Restricted Access Overview
2B: File Creator Questionnaire Checklist

EDRMS Configuration:

3A: EDRMS Basic Configuration
3B: EDRMS Configurating Display Options
3C:Downloading EDRMS Software

EDRMS – Searching:

4A: EDRMS – General Search Methods
4B: EDRMS – Advanced Search Features (Document Content, Complex, Refine, Wildcard, Misc.)
4C: EDRMS – Advanced Search Features (Boolean Searches, String Based Searches)
4D: EDRMS – Searching Features and Functions

EDRMS – Folder Management:

5A: Create Folder in EDRMS
5B: Moving Records in EDRMS
5C: Create Folder in EDRMS – Template
5D: Relating or Cross Referencing Folders in EDRMS
5E: EDRMS Folders – Create Parts
5F: Create Folder References in EDRMS
5G: Information Aid – Create a Folder in EDRMS

EDRMS – Document Management:

6A: Create a Document in EDRMS
6B: Edit a Document in EDRMS

Records Lifecycle and Final Disposition (currently under construction):

Module 7A: Records Lifecycle Overview

Module 7B: Create New Folders in EDRMS for Next Calendar or Fiscal Year and Rollover Processes

Module 7C: Closing E and P Folders in EDRMS

Module 7D: Off-siting Physical Records in EDRMS

Module 7E: Destruction of P Folders in EDRMS

Module 7F: Retrieval and Return of Folders from Storage Facility

Module 7G: Information Aid – Off-site Transfer Checklist

Module 7H: Information Aid – Destructions – On-site Checklist

Managing Emails:

8A: Moving Email Records to EDRMS
8B: Managing Email Checklist

EDRMS – Bulk Moves and Records Deletions (currently under construction):

9A: Bulk Updating Records in EDRMS

9B: Requesting Deletion of Records in EDRMS

9C: Digitizing Records, Redundant and Transitory Records Schedule Processes

EDRMS – Reports (currently under construction):

10A: Printing Reports in EDRMS

10B: Exporting EDRMS Reports to Excel

10C: Cleaning Up Program Files in EDRMS

EDRMS Resources

11A: EDRMS Resources

Destruction Tracker 2023 (FILES)

C&E - LCL_Compliance		TOTALS
ROTT		
Formal	3704	3704
Totals	**3704**	**3704**

Destruction Tracker 2023 (GB)

C&E - LCL_Compliance		TOTALS
ROTT		
Formal	6.1749	6.175
Totals	**6.1749**	**6**

Destruction Tracker 2023 (FILES)

C&E - LCL_Compliance		TOTALS
ROTT	277	277
Formal	31	31
Totals	308	308

Destruction Tracker 2023 (GB)

C&E - LCL_Compliance		TOTALS
ROTT	3.41	3.41
Formal		
Totals	3.41	3

LCRB Destruction Tracking 2022 (File Count)

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTALS
													0
													0
LCL_ManagementServices & HR			**18895**	**6947**	**11476**	**7598**	**3262**						**48178**
LCL_POLCOM							**2875**	**4141**	**7005**			12810	**26831**
													0
Daily Totals	**0**	**0**	**18895**	**6947**	**11476**	**7598**	**6137**	**4141**	**7005**	**0**	**0**	**12810**	**75009**

LCRB Destruction Tracking 2022 (GB - Electronic Storage)

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTALS
													0
													0
LCL_ManagementServices & HR			**73**	**50**	**11**	**8**	**4.07**						**146.07**
LCL_POLCOM							**3.224**	**7**	**8**			11	**29.224**
												10.1	10.1
Daily Totals	**0**	**0**	**73**	**50**	**11**	**8**	**7.294**	**7**	**8**	**0**	**0**	**21.1**	**185**

GB P/ Unit s. 17
Annual SV

LCRB Destruction Tracking 2023 (File Count)

	Jan	Feb	Mar	Apr 18	May 8	Jun 8	Jul 12	Aug	Sep	Oct	Nov	Dec	TOTALS
LCL_Compliance							2717			1865		1839	6421
LCL_Staffinfo					2903	31							2934
LCL_Referencedata						6267							**6267**
LCL_Communications	3302	9289											**12591**
LCL_ManagementServices								363	25				**363**
LCL_Gmshared			2517	1084	933	3902							8436
Daily Totals	**3302**	**9289**	**2517**	**1084**	**3836**	**10200**	**2717**	**363**	**25**	**1865**	**0**	**1839**	**37012**

LCRB Destruction Tracking 2022 (GB - Electronic Storage)

	Jan	Feb	Mar	Apr 18	May 8	Jun 8	Jul 12	Aug	Sep	Oct	Nov	Dec	TOTALS
LCL_Compliance							1.861			0.1415		4.1724	6.1749
LCL_Staffinfo					5	0.322							5.322
LCL_Referencedata						4							4
LCL_Communications	2.34	11.52	1										14.86
LCL_ManagementServices								0.134	0.185				0.319
LCL_Gmshared				0.26	0.57	0.725							1.555
Daily Totals	**2**	**11.52**	**1**	**0.26**	**5.57**	**5.047**	**1.861**	**0.134**	**0.185**	**0.1415**	**0**	**4.1724**	**32**

GB P/ Unit s. 17

MultX1 **Annual SV**

LCRB Destruction Tracking 2023 (File Count)

	Jan	Feb	Mar	Apr 18	May 8	Jun 8	Jul 12	Aug	Sep	Oct	Nov	Dec	TOTALS
LCL_Compliance	308												308
LCL_Staffinfo													0
LCL_Referencedata													**0**
LCL_Communications													**0**
LCL_ManagementServices	2599												2599
LCL_Gmshared													0
Daily Totals	**2907**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2907**

LCRB Destruction Tracking 2022 (GB - Electronic Storage)

	Jan	Feb	Mar	Apr 18	May 8	Jun 8	Jul 12	Aug	Sep	Oct	Nov	Dec	TOTALS
LCL_Compliance	3.41												3.41
LCL_Staffinfo													0
LCL_Referencedata													0
LCL_Communications													0
LCL_ManagementServices	8												8
LCL_Gmshared													0
Daily Totals	**11**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**11**

GB P/ Unit s. 17

MultX1 **Annual SV**

Management Services Destruction Tracking March 2022

Management Services	1	2	3	4	7	8	9	10	11	12	14	15	16	17	18	21	22	23	24	28	29	30	31	TOTALS
HR																								0
Finance																		9						9
Facilities																					51			51
Management Services																						55		55
Admin																		12675	3286	115	1552		1152	18780
Daily Totals	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**12684**	**3286**	**115**	**1603**	**55**	**1152**	**18895**

Annual s. 17

Management Services Destruction Tracking March 2022

Management Services	1	2	3	4	7	8	9	10	11	12	14	15	16	17	18	21	22	23	24	28	29	30	31	TOTALS
HR																								0
Finance																		1						1
Facilities																					1.74			1.74
Management Services																						0.29		0.291
Admin																		46	9.25	0.32	10.23		3.1	68.9
Daily Totals	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**47**	**9**	**0.32**	**11.97**	**0.29**	**3.1**	**72**

Annual s. 17

Destruction Tracker April 2022 (FILES)

Management Services	1	4	5	6	7	8	11	12	13	14	15	18	19	20	21	22	25	26	27	28	29		TOTALS
HR									3														3
Finance																							0
Facilities			151																	43			194
Mgt Services							100	196					70	31	114			223	437				1171
Training						110																	110
Admin	547		30	38	45			570		4200			39										5469
Daily Totals	**547**	**0**	**181**	**38**	**45**	**110**	**100**	**766**	**3**	**4200**	**0**	**0**	**109**	**31**	**114**	**0**	**0**	**223**	**437**	**43**	**0**	**0**	**6947**

Annual s. 17

Destruction Tracker April 2022 (GB)

Management Services	1	4	5	6	7	8	11	12	13	14	15	18	19	20	21	22	25	26	27	28	29		TOTALS
HR									10														10
Finance																							0
Facilities			0.55																	0.26			0.811
Mgt Services							0.85	0.15					1.38	0.39	0.33			0.46	1.83				5.392
Training						0.55																	0.55
Admin	0.85		0.43	0.11	0.6			0.81		30.19			0.4										33.391
Daily Totals	**1**	**0**	**0.98**	**0.11**	**0.6**	**0.55**	**0.85**	**0.96**	**10**	**30.19**	**0**	**0**	**1.78**	**0.39**	**0.33**	**0**	**0**	**0.46**	**2**	**0.26**	**0**	**0**	**50**

Annual s. 17

Cell: J5

Note: Webster, Richard CITZ:EX:
10MB

Destruction Tracker May 2022 (FILES)

Management Services	2	3	4	5	6	9	10	11	12	13	16	17	18	19	20	24	25	26	27	30	31		TOTALS
HR																							0
Finance							146		137	139	927	1915	1118	1516						51	1262		7211
Facilities	2685	27	204	172	315	810																	4213
Mgt Services																							0
Training	32																						32
Admin	20																						20
Daily Totals	2737	27	204	172	315	810	146	0	137	139	927	1915	1118	1516	0	0	0	0	0	51	1262	0	11476

Destruction Tracker May 2022 (GB)

Management Services	2	3	4	5	6	9	10	11	12	13	16	17	18	19	20	24	25	26	27	30	31		TOTALS
HR																							0
Finance							0.17		0.1	0.092	0.825	1.71	1.01	1.45						0.05	1.13		6.534
Facilities	2.18	0.18	0.7	0.202	0.29	0.779																	4.335
Mgt Services																							0
Training	0.012																						0.012
Admin	0.031																						0.031
Daily Totals	2	0.18	0.7	0.202	0.29	0.779	0.17	0	0.1	0.092	1	1.71	1.01	1.45	0	0	0	0	0	0.05	1.13	0	11

Destruction Tracker June 2022 (FILES)

Management Services	1	2	3	6	7	8	9	10	13	14	15	16	17	20	21	22	23	24	27	28	29	30	TOTALS
HR																		1675	167	1592			3434
Finance		1009			2077	967	101																4154
Facilities																							0
Mgt Services				10																			10
Training																							0
Admin																							0
Daily Totals	0	1009	0	10	2077	967	101	0	0	0	0	0	0	0	0	0	0	1675	167	1592	0	0	7598

Destruction Tracker June 2022 (GB)

Management Services	1	2	3	6	7	8	9	10	13	14	15	16	17	20	21	22	23	24	27	28	29	30	TOTALS
HR																		2.03		1.94			3.97
Finance																							0
Facilities		0.96																					0.96
Mgt Services				0.005	1.98	0.98	0.14																3.105
Training																							0
Admin																							0
Daily Totals	0	0.96	0	0.005	1.98	0.98	0.14	0	0	0	0	0	0	0	0	0	0	2.03	0	1.94	0	0	8

Destruction Tracker June 2022 (FILES)

Management Services	4	5	6	7	8	11	12	13	14	15	18	19	20	21	22	25	26	27	28	29	30	31	TOTALS
HR	3262																						3262
Finance																							0
Facilities																							0
Mgt Services																							0
Training																							0
Admin																							0
Daily Totals	3262	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3262

Destruction Tracker June 2022 (GB)

Management Services	4	5	6	7	8	11	12	13	14	15	18	19	20	21	22	25	26	27	28	29	30	31	TOTALS
HR	4.07																						4.07
Finance																							0
Facilities																							0
Mgt Services																							0
Training																							0
Admin																							0
Daily Totals	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4

Destruction Tracker 2022-2023 (FILES)

Management Services		TOTALS
		0
		0
ROTT	153	153
Formal	210	210
		0
		0
Totals	**363**	**363**

Destruction Tracker 2022-2023 (GB)

Management Services		TOTALS
		0
		0
ROTT	0.0903	0.0903
Formal	0.0475	0.0475
		0
		0
Totals	**0.1378**	**0**

Destruction Tracker 2022-2023 (FILES)		
Management Services		TOTALS
		0
		0
ROTT	25	25
Formal		
		0
		0
Totals	25	25

Destruction Tracker 2022-2023 (GB)		
Management Services		TOTALS
		0
		0
ROTT	0.0185	0.0185
Formal		0
		0
		0
Totals	0.0185	0

Destruction Tracker 2023-2024 (FILES)

Management Services		TOTALS
		0
		0
ROTT		0
Formal	388	388
		0
		0
Totals	388	388

Destruction Tracker 2022-2023 (GB)

Management Services		TOTALS
		0
		0
ROTT	0.319	0.319
Formal		0
		0
		0
Totals	0.319	0

Destruction Tracker 2023-2024 (FILES)

Management Services		TOTALS
		0
		0
ROTT	168	168
Formal	2431	2431
		0
		0
Totals	**2599**	**2599**

Destruction Tracker 2022-2023 (GB)

Management Services		TOTALS
		0
		0
ROTT	0.0958	0.0958
Formal	7.8252	7.8252
		0
		0
Totals	**7.921**	**8**

From: Gbenusola, James LCRB:EX
To: LCRB All
Subject: Records Management: Tidy Up your Outlook with Lola!
Date: September 13, 2023 8:15:09 AM
Attachments: image001.png

Tidy Up Outlook with Lola!

Keeping Our Outlook Clean and Efficient

Week One: Using the Cleanup Tool

Your challenge: Keep a tidy inbox by trying the "clean up" function in outlook

Some background

Information is one of our most valuable assets. Having the right information at the right time supports effective decision-making, planning and program/service delivery, and increases public confidence in our work. As public servants, we're all responsible for collecting, managing, and safeguarding information in the form of records. One of the best ways we can do this is by following good records management practices.
Over the next 5 weeks, you will receive tips and action items to improve your records management habits.
Part of records management is knowing what to keep and what to get rid of. Storing digital and paper copies of files costs the Government of British Columbia hundreds of thousands of dollars in taxpayer money every year. Over the past year alone, the LCRB Records and FOI team has destroyed over 100,000 digital files and 1,500 boxes of paper, which will save the branch abou s. 17 a year going forward.

Additionally, managing our records effectively also helps us keep our FOI processes efficient. This is important because all ministries have a duty to be transparent and accountable to the public under the Freedom of Information and Protection of Privacy Act (FOIPPA). You can reach out to the Records and FOI team at lclb.foi@gov.bc.ca for more information about FOI requests or FOIPPA.

Once the cleanup is complete, it is up to us to keep things tidy. Managing your Outlook inbox is a great way to help us achieve our records management goals. That's why, with the help of our mascot Lola, I will be sending weekly challenges for five weeks with simple things you can do to maintain your records in outlook.

Lola is a Green Cheeked Conure and is companion to one of our records team members.

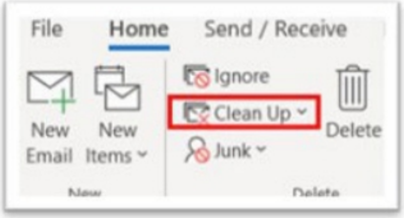
What this means for you and your inbox

Did you know that when an FOI request is submitted, your inbox may be searched for records? This means that you must go through every undeleted email to find relevant information.
Keeping your inbox tidy will save you time and make it easier to find information you need.
One simple thing you can do to shrink your inbox is to use the cleanup tool in your outlook. This cleans up

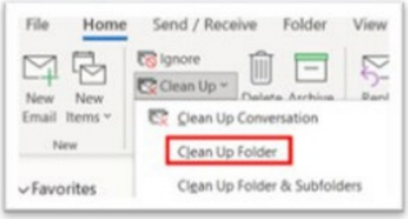
redundant emails such as email chains you were cc-ed on.

It's easy, all you need to do is:

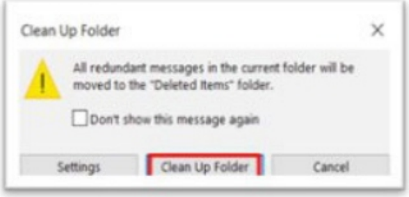
1. Open your outlook email inbox
2. On the top of the screen underneath "home" click on "clean up":



3. Click on "clean up folder":



4. A pop-up will appear, click on "clean up folder"


Clean Up Folder

All redundant messages in the current folder will be moved to the "Deleted Items" folder.

☐ Don't show this message again

5. Your redundant messages will be moved to your "deleted" folder. Look there to see what was deleted.

To learn more about how to use the cleanup tool, click here.

-

For questions around keeping a tidy inbox or records management in general, contact: lclb.foi@gov.bc.ca
We would love to hear from you, please complete a survey on this email series by holding on the link below:
https://forms.office.com/r/AHD6tVseb0

We are writing to you from the territory of the ləkʷəŋən People, which includes the Esquimalt and Songhees First Nations. Want to learn more about creating your own territorial acknowledgement? The Guide to Territorial Acknowledgements will help you get started.

BRITISH COLUMBIA
BC Public Service
Where ideas work

James Gbenusola, CPA, CGA
Manager, Finance and Administration
Management Services | Liquor and Cannabis Regulation Branch
Ministry of Public Safety and Solicitor General
P:778.698.8121 | C: 250.208.1150 | James.Gbenusola@gov.bc.ca
Warning: This email is intended only for the use of the individual or organization to whom it is addressed. It may contain information that is privileged or confidential. Any distribution, disclosure, copying, or other use by anyone else is strictly prohibited. If you have received this in error, please telephone or e-mail the sender immediately and delete the message.

From: Gbenusola, James LCRB:EX
To: LCRB All
Subject: Week Two: Tidy Up your Outlook with Lola!
Date: September 20, 2023 8:36:22 AM
Attachments: image001.png
image007.png

Tidy Up Outlook with Lola!

Keeping Our Outlook Clean and Efficient

Week Two: Creating Folders

Your challenge this week: Create at least one folder in your inbox!

Some background

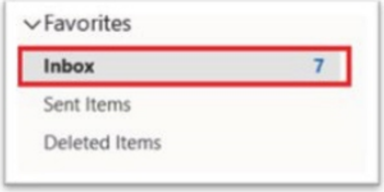
Did you know that you can create folders in your inbox to organize emails?
Use folders to keep personal or transitory emails separate or use folders to identify non-transitory emails. Folders can help make clean up more efficient. (Click here for more information on transitory emails).

What this means for you and your inbox

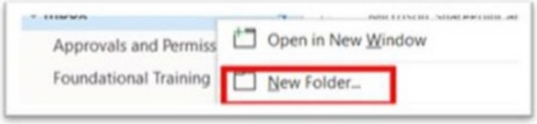
Creating folders can make it easier to find important information in your inbox. It can also help you identify what emails you must save in the LAN.

It's easy, all you need to do is:

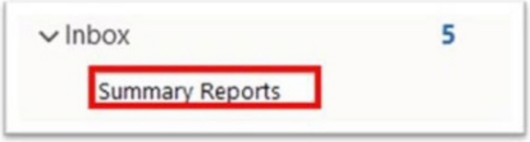
1. On the left panel of your outlook, you'll see your inbox listed:



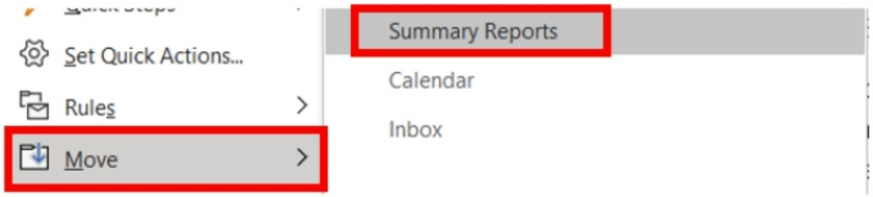
2. Right click on this and select "New Folder":



3. Name your new folder.



4. Now that the folder has been created, return to the main page of your email. Select the email you want to move and right click on it. Select "move" and then click on the folder you want to move the email to.



5. If you create a folder for transitory emails, remember to delete them when you don't need them anymore!

-

For questions around keeping a tidy inbox or records management in general, contact: lclb.foi@gov.bc.ca
We would love to hear from you, please complete a survey on this email series by clicking on the link below:
https://forms.office.com/r/AHD6tVseb0

We are writing to you from the territory of the ləkʷəŋən People, which includes the Esquimalt and Songhees First Nations. Want to learn more about creating your own territorial acknowledgement? The Guide to Territorial Acknowledgements will help you get started.

BRITISH COLUMBIA
BC Public Service
Where ideas work

James Gbenusola, CPA, CGA
Manager, Finance and Administration
Management Services | Liquor and Cannabis Regulation Branch
Ministry of Public Safety and Solicitor General
P:778.698.8121 | C: 250.208.1150 | James.Gbenusola@gov.bc.ca
Warning: This email is intended only for the use of the individual or organization to whom it is addressed. It may contain information that is privileged or confidential. Any distribution, disclosure, copying, or other use by anyone else is strictly prohibited. If you have received this in error, please telephone or e-mail the sender immediately and delete the message.

From: Gbenusola, James LCRB:EX
To: LCRB All
Subject: Week Three: Tidy Up your Outlook with Lola!
Date: September 27, 2023 8:16:31 AM
Attachments: image001.png
image003.png

Tidy Up with Lola!

Keeping Our Outlook Clean and Efficient

Week Three: Sent and Deleted Folders

Your challenge this week: Clean up your sent and deleted folders!

Some background

Did you know that it costs s. 17 per gigabyte per month to store digital information including email?
Our folders can accumulate lots of unnecessary clutter, including deleted and sent emails.
Tidy folders will help you find information more easily, save the branch money, and help the FOI team respond to requests. Click here for more information on FOI requests.
While it's important to keep a record of important conversations, unnecessary emails can accumulate over time, making it harder to find what we need when we need it. This is called Transitory Information.
Transitory emails include information of temporary usefulness that is only needed to complete a routine action or prepare a subsequent record (e.g., a new version).
Click here for some quick tips on identifying and managing transitory emails.

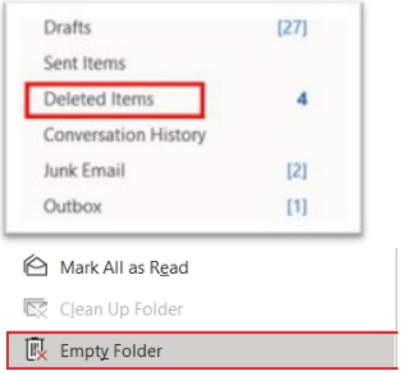
What this means for you and your inbox

Following these suggestions can help you maintain important emails, while clearing up storage space.

It's easy, all you need to do is:

1. **Deleted items folder:**

   Right click on your deleted items folder and select Empty Folder. This can be found on the left side of your inbox in most views:



We often forget to clear this folder; its contents take up valuable storage space and cost money!

2. **Sent items folder:**
   Look through your sent items folder and identify any emails that are no longer required for reference or follow-up (transitory emails).

   Remember, this is not about rushing through the process but rather taking a mindful approach to decluttering while safeguarding important records. Try setting reminders to your outlook calendar once per month, once per week or whatever works for you. For more information on how to add reminders in outlook click here.

-

For questions around keeping a tidy inbox or records management in general, contact: lclb.foi@gov.bc.ca
We would love to hear from you, please complete a survey on this email series by clicking on the link below:
https://forms.office.com/r/AHD6tVseb0

We are writing to you from the territory of the lək̓ʷəŋən People, which includes the Esquimalt and Songhees First Nations. Want to learn more about creating your own territorial acknowledgement? The Guide to Territorial Acknowledgements will help you get started.

BRITISH COLUMBIA
BC Public Service
Where ideas work

James Gbenusola, CPA, CGA
Manager, Finance and Administration
Management Services | Liquor and Cannabis Regulation Branch
Ministry of Public Safety and Solicitor General
P:778.698.8121 | C: 250.208.1150 | James.Gbenusola@gov.bc.ca
Warning: This email is intended only for the use of the individual or organization to whom it is addressed. It may contain information that is privileged or confidential. Any distribution, disclosure, copying, or other use by anyone else is strictly prohibited. If you have received this in error, please telephone or e-mail the sender immediately and delete the message.

From: Gbenusola, James LCRB:EX
To: LCRB All
Subject: Week Four: Tidy Up your Outlook with Lola!
Date: October 4, 2023 8:56:29 AM
Attachments: image001.png

Tidy Up with Lola!

Keeping Our Outlook Clean and Efficient

Week Four: Adding colour categories

Your challenge this week:
Add colour categories to three emails in your inbox!

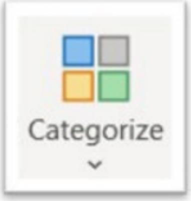
What this means for you and your inbox

You receive dozens of emails every week, and it's easy for important messages to get lost. By assigning colours to categorize emails, we can easily identify non-transitory messages that will require filing later into ORCS and ARCS folders.

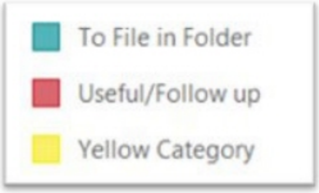
Sticking to a colour scheme will help you associate certain colours with specific types of emails. This will help you easily spot emails that need your attention.

It's easy, all you need to do is:

1. Open outlook and locate an email you want to categorize.
2. With the email selected, go to the tool bar at the top and find the "categorize" button:



3. Click on "categorize" and choose a colour to represent the importance or category of the email. For example, blue for urgent, green for follow-up, purple for personal etc.



For more information on creating and assigning colour categories, click here.

-

For questions around keeping a tidy inbox or records management in general, contact: lclb.foi@gov.bc.ca
We would love to hear from you, please complete a survey on this email series by clicking on the link below:
https://forms.office.com/r/AHD6tVseb0

We are writing to you from the territory of the ləkʷəŋən People, which includes the Esquimalt and Songhees First Nations. Want to learn more about creating your own territorial acknowledgement? The Guide to Territorial Acknowledgements will help you get started.

BRITISH COLUMBIA
BC Public Service
Where ideas work

James Gbenusola, CPA, CGA
Manager, Finance and Administration
Management Services | Liquor and Cannabis Regulation Branch
Ministry of Public Safety and Solicitor General
P:778.698.8121 | C: 250.208.1150 | James.Gbenusola@gov.bc.ca

Warning: This email is intended only for the use of the individual or organization to whom it is addressed. It may contain information that is privileged or confidential. Any distribution, disclosure, copying, or other use by anyone else is strictly prohibited. If you have received this in error, please telephone or e-mail the sender immediately and delete the message.

From: Gbenusola, James LCRB:EX
To: LCRB All
Subject: Week Five: Tidy Up Your Outlook with Lola!
Date: October 11, 2023 9:47:01 AM
Attachments: image001.png

Tidy Up Outlook with Lola!

Keeping Our Outlook Clean and Efficient

Week Five: Deleting Transitory Emails

Your challenge this week:
Find and delete three transitory emails in your inbox!

Some Background:

Did you know that FOI applicants need to pay per page? When we provide them with irrelevant and transitory information, it costs them more money and makes it harder for them to find the information they're looking for. Transitory emails are messages (including attachments) that are only of short-term use and are not needed to document a decision or action.

This also includes:

- Duplicate emails
- Rough notes or incomplete information
- Unused information for the purpose of creating other documents
- Working material used to support projects and develop official records sometimes made during brainstorming and collaboration

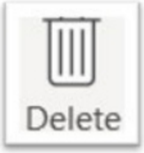
Click here for more information on transitory information.

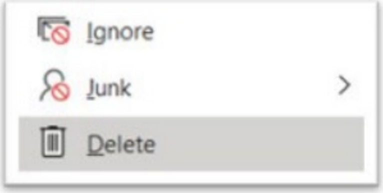
What this means for you and your inbox

Deleting transitory emails saves space in your inbox and money for the branch, taxpayers, and FOI applicants (who pay per page). It also makes information easier to find.

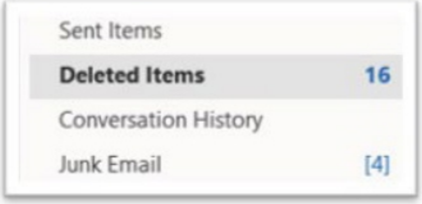
It's easy, all you need to do is:

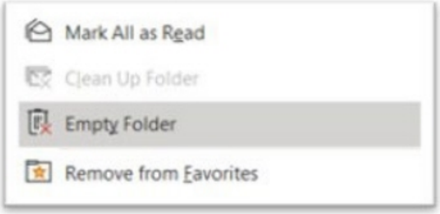
1. Click on the email you want to delete and select the "delete" icon with the trash bin, or right click the email and select delete





2. Deleted emails are moved into your deleted items folder. Be sure to also delete these emails by right clicking on the "deleted items" folder and then selecting "empty folder"





-

For questions around keeping a tidy inbox or records management in general, contact: lclb.foi@gov.bc.ca
We would love to hear from you, please complete a survey on this email series by clicking on the link below:
https://forms.office.com/r/AHD6tVseb0

We are writing to you from the territory of the ləkʷəŋən People, which includes the Esquimalt and Songhees First Nations. Want to learn more about creating your own territorial acknowledgement? The Guide to Territorial Acknowledgements will help you get started.

James Gbenusola, CPA, CGA
Manager, Finance and Administration
Management Services | Liquor and Cannabis Regulation Branch
Ministry of Public Safety and Solicitor General
P:778.698.8121 | C: 250.208.1150 | James.Gbenusola@gov.bc.ca
Warning: This email is intended only for the use of the individual or organization to whom it is addressed. It may contain information that is privileged or confidential. Any distribution, disclosure, copying, or other use by anyone else is strictly prohibited. If you have received this in error, please telephone or e-mail the sender immediately and delete the message.