Yukon Information and Privacy Commissioner

PRIVACY COMPLIANCE AUDIT

Pursuant to Subsection 111(1) of the *Access to Information and Protection of Privacy Act*

Physical Records Destruction Process

File ATP-CMP-2023-02-074

Department of Highways and Public Works

Jason Pedlar, Information and Privacy Commissioner

Aidan Bell, Investigator

Joni Ellerton, Investigator

May 15, 2024

Summary

This compliance audit focuses on the Department of Highways and Public Works' physical records destruction process, and its compliance with the requirements of the ATIPPA and the Regulation, including:

a. Records classification;

b. The administrative, technical, and physical security measures put in place to protect personal information;

c. Measures to protect the personal information against risks of theft, loss, or unauthorized use, access, and disclosure.

The Information and Privacy Commissioner conducted a compliance audit and found the following:

- There are several inherent risks in the Department's physical records destruction process.

- The Department did not establish that their method of classifying records is compliant with the classification requirements in section 9 of the Regulation.

- The Department has a clearly defined process for the general physical records destruction process, but it has not been recorded in a written format in accordance with its obligations under section 30 of the ATIPPA and section 9 of the Regulation.

- The Department has several subsidiary processes for physical records destruction that are not clearly defined and did not demonstrate that it is protecting personal information in accordance with its obligations under 30 of the ATIPPA and section 9 of the Regulation.

As such, the Information and Privacy Commissioner made six recommendations to remedy these issues.

Table of Contents

Jurisdiction

The IPCs authority to conduct compliance audits is set out as follows.

> *111(1) In addition to the Commissioner's other powers under this Act, the Commissioner may…*
>
> *(b) conduct, in accordance with subsection (2) and the regulations, if any, a privacy compliance audit of a public body for the purpose of assessing the public body's exercise of a power, or performance of a duty, under a provision of Part 2, including*
>
> *(i) the public body's provision of a personal identity service, or*
>
> *(ii) the public body's management of the personal information that it holds;*

Statutes and Regulations Cited

Access to Information and Protection of Privacy Act, SY 2018, c.9

Access to Information and Protection of Privacy Regulation, OIC 2021/025

Explanatory Note

All section references in this report (Report) are to the *Access to Information and Protection of Privacy Act* (ATIPPA), unless otherwise stated.

Introduction

Public bodies must have authority under the *Access to Information and Protection of Privacy Act* (ATIPPA*)* and the *Access to Information and Protection of Privacy Regulation* (Regulation) to collect, use and disclose personal information. Public bodies are also obligated to adequately secure personal information in their custody or control.

Given the privacy risks associated with an inadequate physical records destruction process, the IPC felt it was appropriate to examine the Department of Highways and Public Works' policies, procedures, and practices. On February 13, 2023, the IPC initiated a privacy compliance audit (Compliance Audit).

This report provides an overview of the legal framework relevant to the secure destruction of physical records, discusses the Department's processes for destroying physical records, and assesses how those processes comply with the requirements of the ATIPPA and the Regulation.

Background

On February 13, 2023, the IPC issued a Notice to Produce Records (NTPR) to the Department.

On March 7, 2023, the IPC received the Department's response to the NTPR including the Department's policies, procedures, forms, and guidance documents relating to the disposal process of documents that may contain personal information. Our office engaged with the Department through email to further clarify what each document submitted to us was explaining regarding their document destruction process.

On May 10, 2023, the IPC conducted a site visit at both the Records Centre and the Document Destruction Centre.

The conclusions, recommendations and observations of this Compliance Audit are based on the information provided in the Department's response to the NTPR, including subsequent exchanges and information gathered during the site visits.

Scope of Compliance Audit

This compliance audit focuses on the Department of Highways and Public Works' physical records destruction process, and its compliance with the requirements of section 30 of the ATIPPA and the relevant sections of Regulation, including:

a. Records classification;

b. The administrative, technical, and physical security measures put in place to protect personal information;

c. Measures to protect the personal information against risks of theft, loss, or unauthorized use, access, and disclosure.

Records Life cycle

Destroying records is essential to maintaining effective records systems. All records have some practical period of usefulness. The decision to keep a record permanently as part of a historic archive, for example, or to destroy it at a pre-determined point in time is based on the utility of the record to the organization.

This is best explained as a record life cycle made up of four stages: create, maintain, store, and dispose of:

1. Create - Records are created in the use of everyday standard work processes. Some of those records may be recycled immediately if they don't contain personal information (PI) or may be considered transitory records with no long-term relevance and must be destroyed in a method that ensures secure destruction.
2. Maintain – Items like working documents or drafts may need to be maintained in the evolution of a final document.
3. Store – The final document produced from work may need to be filed or stored for a predetermined retention period as per the Department's records retention policy.
4. Dispose - Ensuring the safe disposal of records, considering potential risk of significant harm to affected individuals from a privacy breach, is crucial for the efficient operation of a department and the protection of individuals' PI.

A retention period, also called a "records schedule", is a part of the record life cycle. It describes how long an organization needs to keep a record, where it's stored, and how to dispose of the record when it has reached it destruction date. Destruction is the final stage in the record life cycle. The process or method of destruction will vary based on the type or class of PI contained in the record and the risk of harm associated with each record.

It is imperative for every public body to establish a written policy that clearly outlines the circumstances under which record destruction is appropriate.

Once records have surpassed their practical usefulness, a decision must be made whether to retain them according to a records retention policy or proceed with their destruction. This decision guarantees that the public body's records remain up-to-date and relevant.

Implementing a records destruction process is essential to maintaining the credibility and easy accessibility of a public body's records. Failure to do so can lead to privacy breaches through disorganization and the unnecessary retention of a large volume of records.

Legal Framework

If information is not destroyed in a secure manner, it may be accessed by a third party. Under s.23, any disclosure of personal information that is not provided for under the ATIPPA, or that is beyond the amount that is reasonably necessary, is unauthorized. The unauthorized disclosure of personal information can result in embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, and in some cases, a risk to personal safety.

To safeguard against these risks, s.30 of the ATIPPA states that, *"The head of a public body must protect personal information held by the public body by securely managing the personal information in accordance with the regulations."* s.30 of the ATIPPA assigns the responsibility of safeguarding personal information held by a public body to its Minister, and the Regulation sets out the way in which information is to be safeguarded.

The following provisions of the Regulation apply to this audit:

> *s.9(2) For the purpose of section 30 of the Act, the head of each public body must establish and implement administrative, technical and physical security measures appropriate to protect the personal information of each type or class of personal information that it holds.*
>
> *s.9(3) The security measures established under subsection (2) must include the following:*
> *(b) measures to protect the personal information against risks*
> *(ii) of damage, corruption or unintended destruction*
> *(iv) of unsecured storage, transmittal or transfer,*
> *(v) of theft, loss or unauthorized use, disclosure or disposal, and*
>
> *s.9(4) In establishing and implementing security measures under subsection (2), the head of a public body must take the following into account:*
> *(a) the types or classes of personal information that it holds;*
> *(b) the sensitivity of the personal information of each type or class of personal information that it holds;*
> *(c) for each type or class of personal information that it holds, the risk of harm, including significant harm, that may occur to an individual if the public body fails to protect the personal information;*
> *(d) the benefits and costs of alternative security measures.*

The above requires that the public body have a policy in place that ensures records are identified and stored based on the classification of PI they contain. See the Records Classification section of this report). The policy must identify the risk of harm each class may

pose if a privacy breach were to occur. Such records should be stored in a facility that the public body has deemed to have security measure standards to prevent a breach of privacy. Security measures must encompass the storage and transportation of such records to their final destruction point.

The Regulation continues:

> *s.9(13) In addition to meeting the requirements of subsections (2) to (6), (8) and (10) to (12), the head of each Class A public body must, with respect to the public body,*
>
> *(a) establish or adopt written policies respecting the protection of the personal information held by it;*
>
> *(b) ensure that the effectiveness of its security measures is tested and evaluated on a periodic basis;*
>
> *(c) modify its security measures as required to ensure the protection of the personal information held by the public body;*
>
> *(d) update its security measures when necessary to comply with the Act and this Regulation;*
>
> *(e) establish a written information security strategy regarding the establishment and implementation of security measures under subsection (2) and the establishment of policies under paragraph (a);*
>
> *(i) set out practices and procedures to effectively mitigate against risks to the secure management of the personal information that it holds that may arise from a service provider being given access to personal information held by it.*

Section 9(13) speaks to a public body's requirements for a policy and step-by-step procedure that it provides for their employees to ensure they understand how to identify the different classes of PI and keep them updated with changes to such procedures.

To comply with s.30, and s.9 of the Regulation, public bodies must adequately protect the personal information they hold.

Records Classification

Records classification is the process of organizing records into categories based on their type, content, or other characteristics. This helps to improve the efficiency and effectiveness of managing, storing, and accessing the records, and to ensure that they are properly protected, preserved, and destroyed.

Typically, records are classified according to a predetermined set of rules or criteria, such as their business value, legal requirements, or retention periods. This allows organizations to easily and accurately identify, retrieve, and manage the records they need in a timely manner. Under s.9(4)(a) of the Regulation, the class or type of PI that records contain must be considered when a public body implements security measures.

As part of their obligation under s.9(2) of the ATIPPA, public bodies must have procedures and policies in place for classifying records and for destroying each class of record at the end of their life cycle.

It is for this reason that it is important to have a records classification system. It not only identifies the type or class of PI contained in a record, but also acts a gauge to assess the risk of harm that may occur to individuals in the event of a privacy breach. As the risk of harm associated with the type of PI increases, so do the security measures required to destroy such records.

Transitory records only have short-term use and do not need to be filed. They are produced or received in the course of everyday work, in the preparation of other records which replace them, or for convenient reference. Transitory records could include rough drafts or notes that have been superseded by a later draft or final version. However, they may contain sensitive information and therefore must still be disposed of securely and under the guidance of established policy or procedures that ensure compliance with the ATIPPA and the Regulation.

Non-transitory records include evidence of business transactions, activities and decisions of a public body, and are required for future business, legal or archival purposes. Non-transitory records may contain personal information that is used to make a decision that directly affects an individual and must be retained for at least one year in accordance with s.22(b) of the ATIPPA. Each public body is responsible for creating their own destruction procedures.

A public body may also possess highly sensitive information such as personal medical files, social insurance numbers, or date of birth records. Such records would require a highly secure destruction process. This could include a secure transfer of such records, specific shredding levels, and appointed workers witnessing the shredding of these types of records.

Without a data classification process, an organization may treat all information the same. This may increase the probability that sensitive data will not have adequate security controls and

could increase the risk of sensitive data being compromised. It also means that less sensitive data may have more security controls than necessary, leading to unnecessary restrictions and loss of an organization's operational efficiency. Given that a public body must classify the personal information that it holds, a data classification process is also necessary under the ATIPPA.

Department's Document Destruction Process

Our compliance audit found that the Department has separate processes for the destruction of transitory records and non-transitory records that have reached the end of their life cycle. Both processes engage a secure shredding facility. The Department also had several other processes that were less clearly defined.

This section of the report provides an overview of the following:

- Secure Shredding Facility
- Destruction of Transitory Records
- Destruction of Non-Transitory Records
- Unknown Processes

Secure Shredding Facility

The Department uses a secure shredding facility known as the Document Destruction Centre (DDC), located at [redacted] in Whitehorse. The DDC operates under the Diversity and Inclusion branch of the Public Service Commission (PSC) and provides document destruction services to the Government of Yukon.

The DDC leases an area within [redacted] building secured independently with a separate alarm system. The DDC can only be accessed by DDC staff and authorized Yukon Government employees. Further, a manager from the PSC is always on site to oversee its operation.

Destruction of Transitory Records

Records that are transitory are generally placed into a designated bin as part of a shredding bin program. Non-transitory records are managed through a separate process, as outlined below.

Most of the Department's Whitehorse branches use the DDCs shredding bin program to securely dispose of their transitory records. Each shredding bin is assigned a unique bin and site number by the DDC for tracking and oversight purposes and is delivered locked. Government departments can contact the DDC to pick up a secured bin that is at capacity and exchange it with an empty bin. The shredding bin program operates on a regular schedule including email reminders from the DDC to schedule bin exchanges if necessary. Ad-hoc bin exchanges can be accommodated outside of the fixed schedule, upon request.

Transportation and exchange of the shredding bins, including pick-up and delivery, is contracted out to bonded employees of [redacted]. The shredding bins remain locked throughout the entire transportation life cycle and are only unlocked by the DCC manager when the contents are ready to be shredded at the DDC. The DDC manager is in control of the keys used to unlock the secure bins.

Destruction of Non-Transitory Records

The Records Centre (RC) stores records for all participating government departments according to the records retention schedule of that Department. The RC is operated through the Corporate Information Management branch of the Information and Communications Technology (ICT) division of Highways and Public Works. However, the records are viewed as being in the control of the originating department, even though they are in the custody of the RC.

When a department's on-site retention period expires, the records are sent to the RC. The department informs the RC of the length of time that the records are to be stored, and the RC then monitors the age of the records.

Once received by the RC, records are catalogued, assigned a number, and entered into Infolinx**.** Infolinx is records and information management software that enables Yukon government to track, manage, and audit the complete life cycle of physical records at the file level.

Once records have met their retention period, the RC generates a disposal notice as specified in the Infolinx database. The controlling department then reviews the notice and confirms the records are to be destroyed. After the RC received confirmation, the records are sent to the DDC for destruction.

The method of transportation to the DDC depends on the quantity of records being sent for destruction. [redacted] After the records have been destroyed, the DDC creates a destruction certificate that is issued to the department for their records.

DDC Destruction Process

Records that arrive at the DDC are categorized to indicate the type of material. [redacted]. Any non-recyclable material must be removed to preserve the integrity of the material sent for recycling and protect the shredders from excessive wear and damage. [redacted]

Most paper material is shredded through the strip cut shredder, the MBM DESTROYIT Model 4107 SC. This is considered the primary shredder and is believed to produce better paper (mulch) for recycling. As a result, this is the machine most often used and has a backup machine of the same make and model. This is considered low level security and is useful for general information but not for information that may contain more sensitive information, such as passwords or other sensitive PI.

The second shredder is a cross-cut shredder, the MBM DESTROYIT Model 5009 CC. After destruction, the data can be reproduced only with considerable effort.

The cross-cut machine can be requested by a department for any material that has been identified to contain sensitive data.

Unknown Processes

The Department acknowledged that the above processes do not account for the destruction of all records, and that some processes were less clearly defined.

In some cases, [redacted].

There is no available guidance on the Department's use of its own shredders (rather than the DDC), and as such there is little information available about the security of the shred, storage, and post-shred handling. The number of branches using their own shredder is unknown.

Additionally, the process of record destruction at the Department's branches outside of Whitehorse could not be determined. This audit found that outside of Whitehorse, it has 21 maintenance camps. Out of these branches, 6 indicated they shred paper, and 5 indicated that they burn paper. Details of how the remaining 10 branches destroy records containing PI were not provided by the public body.

As it is not practical for some of the branches outside of Whitehorse to utilize the secure shredding at the DDC, records are likely destroyed by using their own shredders, or by burning them. If a branch is unable to utilize the DDC, the Department does not provide other means of destroying records to the branch.

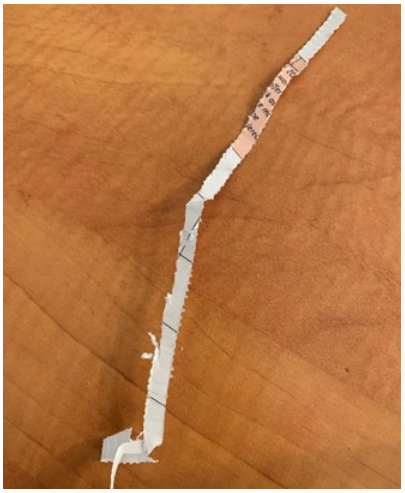
Analysis

This section contains our comments on the compliance of the processes described above. Specifically, we considered whether the Department has adequate physical and administrative security measures in place with respect to the destruction of documents.

Physical Security Measures

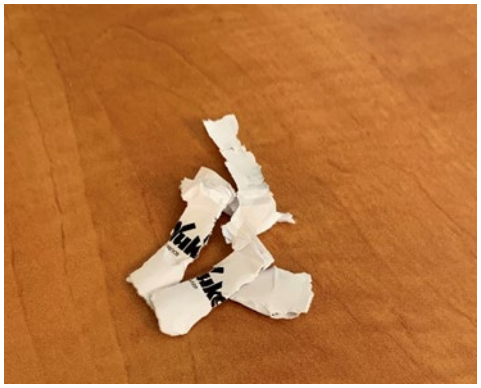
Not all shredders are equally secure. The German Institute for Standardization's DIN 66399 is the worldwide standard for evaluating the security of a shredder. We refer to that standard in this report as the DIN security level. Broadly speaking, shredders producing smaller particles are more secure, as it is more difficult to reconstruct the shredded information. The more secure a shredder, the higher the DIN security level.

The DIN security level of the machines used at the facility may not be sufficient to destroy records in such a way that no personal information is revealed. Transitory records are destroyed using a shredder with a DIN 2 security level, which cuts paper into strips of a maximum width of 6mm, with a maximum size of 800mm². After destruction, the data can be reproduced with a certain degree of effort. Refer to the picture to the left for an example of the shredded material.



While a DIN 2 security level may be suitable for some kinds of information, it is not generally considered to be appropriate for highly sensitive information, as it may be possible to reconstruct documents from the shredded material. This means that there is a risk that highly sensitive personal information may not be adequately disposed of.

Additionally, the cross-cut shredder used for non-transitory records is a DIN 3 security level, which likewise may not be sufficiently secure. A DIN 3 security level shreds an A4 document into 195+ particles of a maximum size of 320mm². Refer to the picture to the right for an example of the shredded material.



After records are shredded, [redacted]

[redacted]. To mitigate this risk, a manager is on-site to supervise the employees. In our view, this is likely an effective deterrent. If a manager is unavailable, video surveillance may be appropriate, and could achieve the same effect. Refer to our report on video surveillance for further information on considerations relevant to the use of video surveillance.

We also note that the shredders are advertised as being capable of shredding non-paper materials (e.g. DVDs, 3-ring binders). With this capability, it may be appropriate to forgo the manual sorting of materials. This may reduce the labour involved and minimize the risk of a privacy breach.

The DDCs shredding bin program has additional security measures in place. For example, the secure bins remain locked throughout transportation, reducing the potential for any unauthorized use or disclosure. [redacted]. This is a control that reduces the likelihood that an unauthorized individual would access the personal information.

Administrative Security Measures

This section of the report considers whether the Department's policies and procedures for destroying records are compliant with the applicable sections of the ATIPPA and the Regulation.

The ATIPPA does not prescribe specific measures, policies, or strategies that a public body must adopt to protect personal information in this context. As described above, the public body must "*establish or adopt written policies respecting the personal information held by it,"* and "*modify its security measures as required."* To determine whether a given security measure is adequate, the *ATIPPA* requires that the public body consider how the information is classified (refer to the section above on data classification) and implement a measure that is "*appropriate to protect the personal information"* of that class. Our office therefore considered whether the administrative measures adopted with respect to the destruction of records (including both transitory and non-transitory records) were appropriate based on their classification.

Following our review of the Department's process for destroying records, it was our view that, while it was able to describe its administrative measures in detail, further written documentation would be required for it to satisfy all its relevant obligations. We also identified some concerns with how records are classified.

An employee of a public body must first determine whether a record is transitory. This underscores the importance of understanding the classification of records. A gap exists in that an employee may incorrectly classify a record as transitory. Employees must understand how to identify records for this process to run effectively. In our view, inaccurately classifying a record

as transitory or non-transitory presents some risk of disposing personal information inappropriately. Whether or not a record follows its life cycle as transitory or non-transitory, it will result in a record being destroyed by a secure shredding machine. However, records classified as transitory are not put through a cross-cut shredder.

Recall that transitory records may still include sensitive personal information. For example, a document containing an individual's personal information may not have been relevant to a public body's work, and the public body may not be obligated to retain it. By classifying records solely based on whether they are transitory, rather than by the class of personal information that the record holds, there is a risk that records containing personal information may be disposed of less securely than records containing no personal information. Conversely, classifying a record inappropriately may result in personal information being retained unnecessarily.

With regards to the classification of records, the Department informed us:

"We do not specify classes of personal information in this manner. The government does not indicate a difference between physical record types. Physical records are either indicated as "destroy" or "appraise/appraisal" for their final disposition under approved retention and disposition authorities. They are not segregated by personal information or non-personal information."

The Department classifies information based on whether it is transitory, which may result in personal information being disclosed in a less secure manner. This also means that it is non-compliant with s.9(2) of the Regulation, which requires that personal information be protected in a manner appropriate to its type or class. As such, we recommend that the Department develop a method of classifying records that comply with the ATIPPA. As an interim measure, requesting the use of a cross-cut shredder for transitory records would help to ensure that personal information on those records is managed more securely.

We found that the Department explained the process associated with the destruction of transitory records in detail. However, our notice to produce records requested written policies and procedures with regards to physical destruction process of materials. No written policy or procedure was provided to us regarding the destruction of transitory records, and the Department confirmed that there is no written policy or process in place regarding the Bin Program (i.e. the destruction of transitory records). In addition, we were informed that it does not regularly audit its physical records destruction process.

It is our view that the Department's process for destroying records does not comply with the requirements found in section 9 of the Regulation relating to written material. To become compliant, the Department must establish written policies and procedures to ensure that employees understand their responsibilities regarding record classification and destruction.

Furthermore, it is crucial that it regularly update, review, and audit these procedures to ensure their effectiveness.

We have recommended that the Department establish a written policy and procedure specifically for staff members on the destruction of records, which should include checklists like those used for the stored records process. Additionally, we suggest that it conduct regular internal audits to evaluate the effectiveness of their written policies regarding the disposal of temporary records. This will help to ensure that the Department satisfies its obligation under s.9(13)(b) of the Regulation to test and evaluate the effectiveness of its security measures on a periodic basis.

Additional Discussion

The Department acknowledged that the above processes do not account for the destruction of all records. Specifically, some branches may destroy records locally (e.g. with their own shredder), and it is unclear what process is followed by branches outside of Whitehorse that do not make use of the DDC when they destroy their records.

While it is possible that those processes are compliant (e.g. if records are destroyed locally in a secure manner with a clearly defined retention schedule and an appropriate classification system), the Department has not, for the purposes of this audit, provided enough information for our office to decide about the compliance of those processes.

Given that the protection of personal information within all branches of the Department is an accountability of the public body head, it is our view that it must consider what measures are appropriate in the scenarios described above and must ensure that written policies are developed to account for these scenarios.

As the focus of this audit was solely on the Department of Highways and Public Works, it is unclear what the practices of other government departments are, and whether they comply with the ATIPPA. To that end, the Information and Privacy Commissioner may exercise his discretion to conduct additional compliance audits in the future.

Conclusions

With respect to the Department's physical security measures, our office concluded that shredders with a higher DIN security level may be appropriate. While there are several risks inherent in the it's process, we believe that effective mitigations are in place.

With respect to the destruction of records, our office concluded that, while the Department has a clearly defined process, this has not been recorded in a written format, contrary to s.9 of the Regulation. It is also our view that it's method of classifying records may not comply with the classification requirements in the ATIPPA.

Additionally, our office found that the Department engages several processes that are not clearly defined. For example, it is unclear how branches outside of Whitehorse dispose of their personal information, or how it manages the use of local shredders. In our view, this must be addressed by developing written policies, and ensuring that the measures taken are appropriate based on the classification of the personal information in the record.

Recommendations

To comply with section 30 of the Act and Section 9 of the regulations, we are also making the following recommendations to the Department:

Recommendation 1: Establish a written policy and procedure for employees on the destruction of records, which should include checklists like those used for the stored records process.

Recommendation 2: Conduct regular internal audits to evaluate the effectiveness of their written policies regarding the disposal of temporary records.

Recommendation 3: Incorporate regular audits at specified intervals to ensure the effectiveness of the record tracking and scheduling process for destruction.

Recommendation 4: Develop a data classification system for the personal information that it holds and reference the appropriate class of personal information in the policies and procedures referred to above.

Recommendation 5: Consider using a cross-cut shredder for transitory records containing sensitive personal information, in addition to the use of a cross-cut shredder for non-transitory records.

Recommendation 6: Assess whether a more secure shredder is appropriate for highly sensitive information.

Department Head's Response to our Privacy Compliance Audit

I am providing the Department Head an opportunity to respond to this Privacy Compliance Audit and notify us whether they are accepting or rejecting each recommendation. We ask that you respond within 15 business days from the date of this Report. Please advise me of your decision on or before June 6, 2024**.**

[redacted]

Aidan Bell
Investigator

[redacted]

Joni Ellerton
Investigator

[redacted]

Jason Pedlar, BA, MA
Information and Privacy Commissioner

Distribution List:

Department Head
Director, Corporate Information Management

Appendix A: Documents Provided by Public Body

Archive Disposition Detailed Process

Bin Location List

Bin Tracking

Box Label Confidential SHRED Record Centre

Box Prep-to-RC-website

Box Transfer-to-RC-website

DDC Destruction Certificate-Sample

Destruction Disposition Process Steps

Destruction Disposition Process-Infolinx 2023

Document Destruction Centre Delivery Form

Document Destruction Centre Process for Paper Material

Transitory records Schedule

Privacy Management Policy

Records Centre Completed Disposal Template

PRIVACY MANAGEMENT POLICY -GAM – POLICY 2.7 – EFFECTIVE October 27, 2015

RecordsCentre-Disposal-SharePointSite_20230227

Information Management Refresh Presentation – Jan 2023

Security of Public Records Policy – Aug 1, 1994

Shredder Info

Transitory Records FAQ-website

Transitory Records Tips-website

What-are-Transitory Records-website