



Lakehead
UNIVERSITY

Data Classification Training & Awareness
Researchers

Table of Contents



Introduction to Data Classification

What is it & why is it important?



Lakehead's Research Data Classification Levels

Overview of the classification levels & examples of data elements



Roles & Responsibilities

How does this apply to your role & what are your obligations?



Data Handling Controls Standard

Overview of the guidelines, including scenario-based guidance



Training Resources & Contact Information

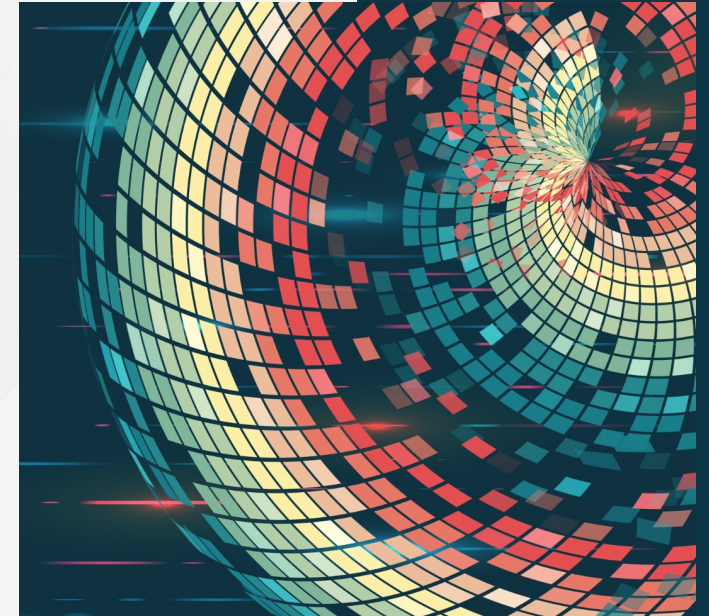
Where to access additional resources & who to contact for support



Q & A Period

Introduction to Data Classification

What is it & why is it important?



Research Data & Understanding Sensitivity

Research data is data that are used as primary sources to support technical or scientific enquiry, research, scholarship, or creative practice, and that are used as evidence in the research process and/or are commonly accepted in the research community as necessary to validate research findings and results.

Research data can contain information that **may require** additional **data handling** and **protection safeguards** in place **due to its sensitivity**. This can include:

Personal Information (PI)

Any information which **relates to a natural person** and **directly or indirectly allows that person to be identified**. This can include:

- First & Last Name
- Date of Birth
- Identification documents (e.g., driver's license, passport)
- Income and financial information

Personal Health Information (PHI)

Any identifiable health information about an individual pertaining to their **mental or physical health**. This can include:

- Health diagnosis
- Health card number
- Family medical history
- Genetic information

Sensitive Information

Information that **entails a high level of reasonable expectation of privacy** due to its **intimate nature** or the **context of its use or communication**. This can include:

- All PI and PHI
- Intellectual property
- Ethnic or racial identity
- Sexual orientation
- Religious or political beliefs

What is data classification?



Data classification will enable you to assign a sensitivity level to research data to identify the appropriate **baseline controls** for **handling and safeguarding** that data.

The **proper classification, management, and protection of research data** at the University helps to ensure:

- ✓ The **quality, integrity, security**, and **authorized accessibility** of **research data**
- ✓ That **research data** is **managed** and **safeguarded in alignment** with **legislative** and **regulatory requirements** and **guidelines**¹

¹ Government of Canada's [Tri-Agency Research Data Management Policy](#) and the [Safeguarding Your Research Guidelines](#)

Research Involving Indigenous Peoples in Canada

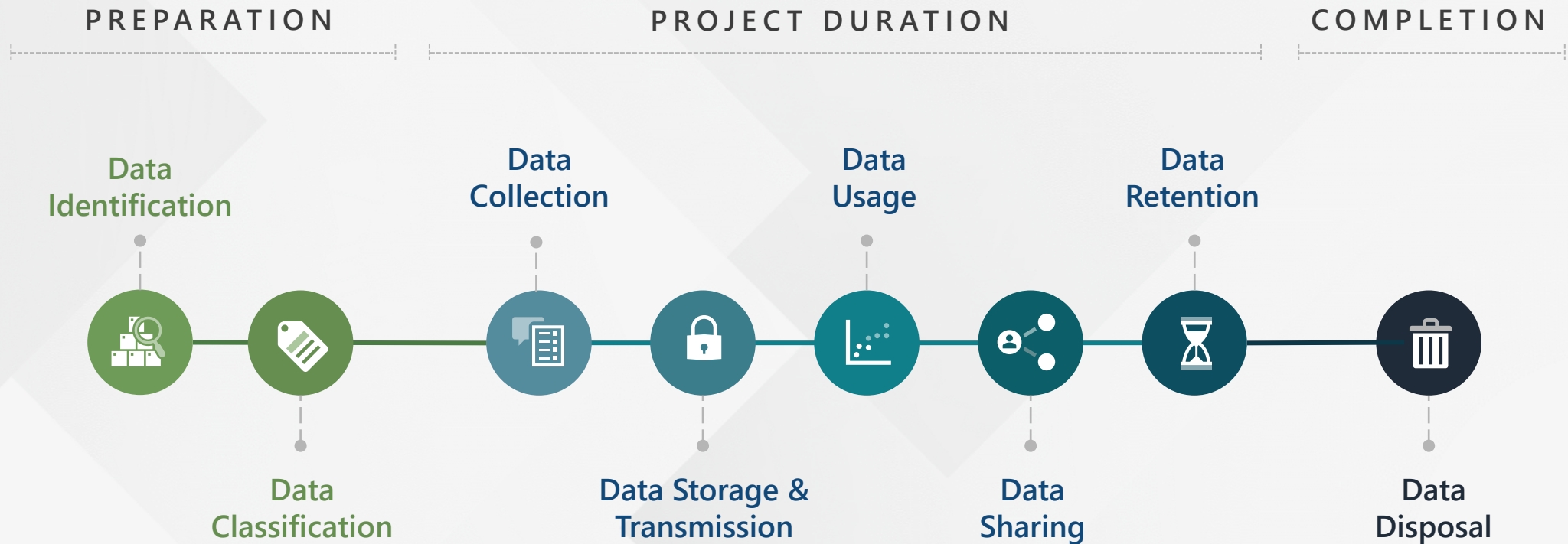
For research involving Indigenous peoples in Canada, ownership of research data is governed by the **First Nations Principles of OCAP®**.

While Lakehead's Research Data Classification Guidelines broadly apply to all University research data, **these guidelines do not supersede the Principles of OCAP®** where research data involves First Nations, Inuit, or Métis participants.

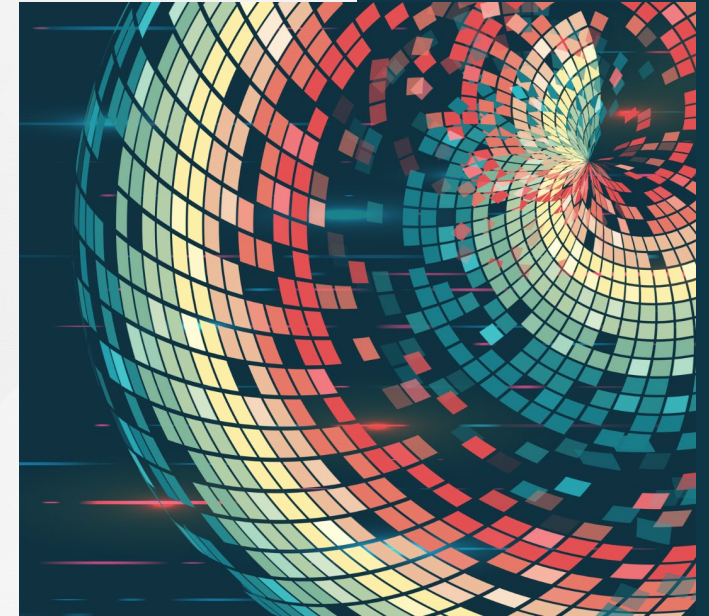


Where divergences exist between the application of OCAP® and Lakehead's Research Data Classification Guidelines, **they should be addressed and resolved** in consultation with the Office of Research Services **prior to the commencement of the research project.**

Research Project Information Lifecycle



Lakehead's Research Data Classification Levels



Lakehead's Research Data Classification Levels

There are three classification levels that research data should be classified under:

Confidential / Sensitive	Internal / Private	Public
<p>Data only available to limited authorized individuals; unauthorized disclosure could result in severe harm to an individual or the University.</p>	<p>Data available to authorized users for research purposes; unauthorized disclosure could result in minor harm to an individual or the University.</p>	<p>Data that is deemed public by legislation or through a University policy; disclosure would not result in any harm to an individual or the University.</p>
<ul style="list-style-type: none"> ❖ Human participants' name, address, health & medical information, income ❖ Intellectual property ❖ Unpublished research data & library transactions 	<ul style="list-style-type: none"> ❖ Research team meeting minutes & correspondence ❖ Contracts between researchers & community partners ❖ Project funders' contact information 	<ul style="list-style-type: none"> ❖ Published research data ❖ Researchers' name and business contact information ❖ Aggregated human subject data (where re-identification is not possible)

What data needs to be classified?



Research data that is within the researcher's control and is within the University's environment

Data hosted within the University's on-premise and cloud systems, including any research data stored on University-provided systems / devices.

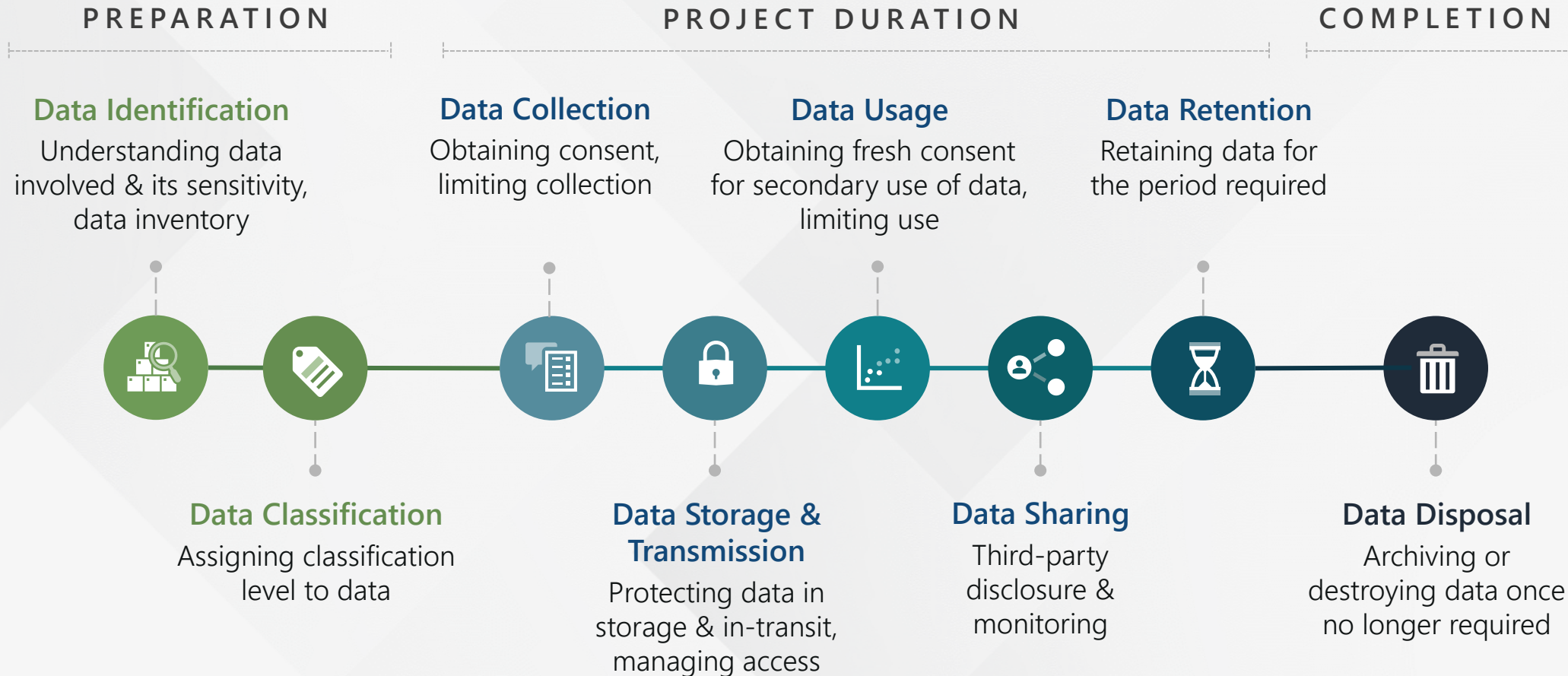


Research data that is stored by a third party outside of the University's control that researchers are provided access to

Research participants' data collected by a hospital or community partner and stored and managed within their respective databases, with access provided to the University's researchers

Research Project Information Lifecycle

Data Classification & Handling Key Steps



Roles & Responsibilities for Classifying & Handling Research Data



Office of Research Services (including Research Facilitators)

- Monitor organizational adherence to the Guidelines and Standard and provide guidance to Principal Investigators and Research Team Members on the Guidelines and Standard
- Review and update the Guidelines and Standard periodically and as there are changes
- Provide data sharing agreement template to researchers



Principal Investigators

- Understand the research data collected and used, the data sensitivity, and how it flows throughout the information lifecycle
- Assign classification to research data
- Identify appropriate controls to implement
- Implement (and/or delegate implementation of) appropriate controls
 - Principal Investigators are responsible for implementing technical controls within systems/applications that are not University-provided or approved by IT



Research Team Members (including Student Researchers)

- Understand the research data involved and their assigned classification
- Implement data handling controls based on the assigned classification



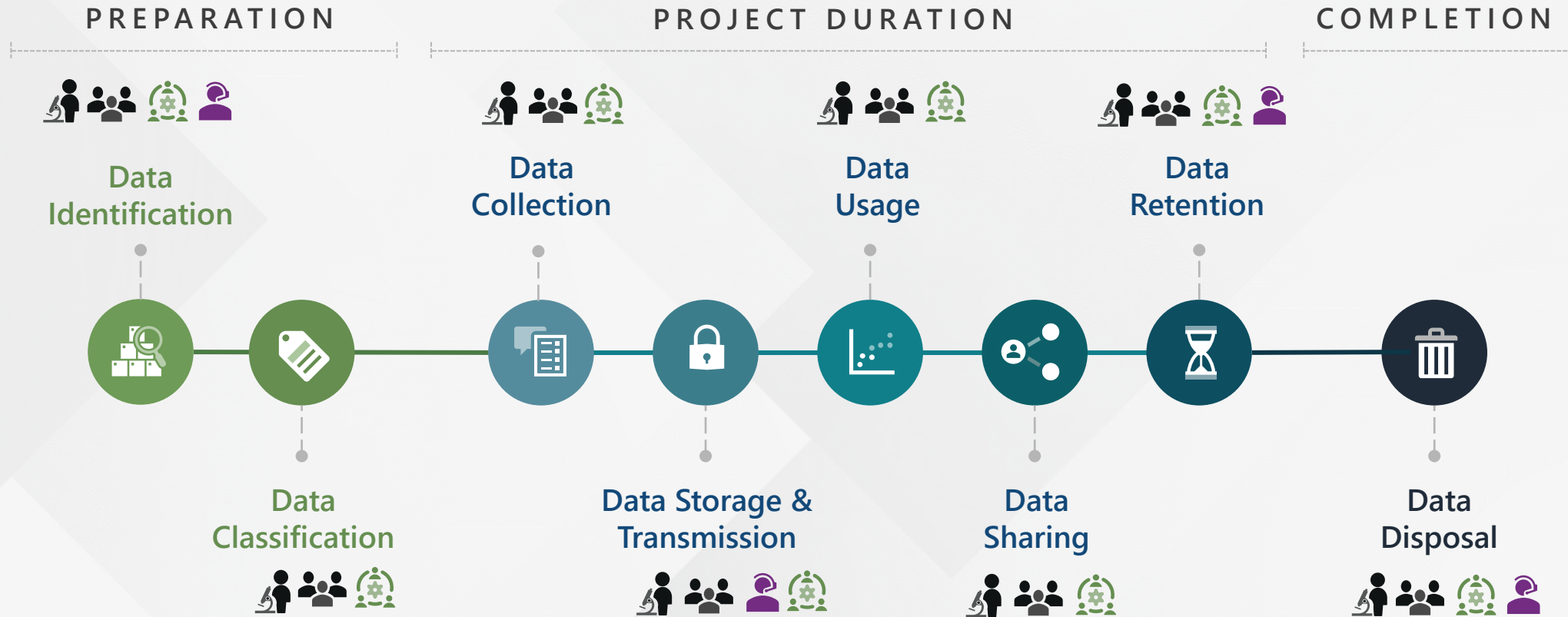
Technology Services department (IT)

- Implement appropriate data handling controls based on the assigned classification within systems / applications that are used for research activities
- Provide support to Principal Investigators and Research Team Members in understanding and implementing technical controls



How does **data classification** apply to you?

Data Classification & the Research Project Information Lifecycle



Possible Stakeholder Involvement



Office of Research Services
(including Research Facilitators)



Principal Investigators

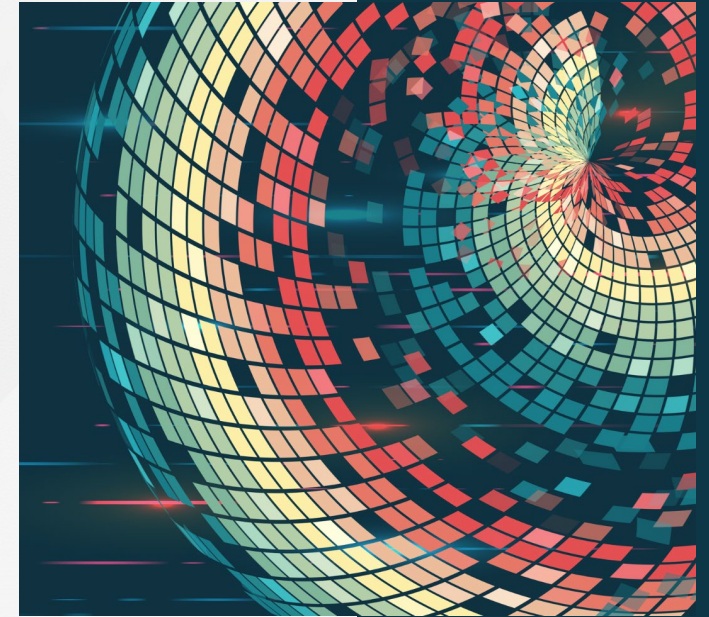


Research Team Members
(including Student Researchers)



Technology Services
department (IT)

Data Handling Controls Standard



Data Classification & the Research Project Information Lifecycle

PREPARATION



Data Identification

Understanding data involved & its sensitivity, data inventory

PROJECT DURATION



Data Collection

Obtaining consent, limiting collection



Data Usage

Obtaining fresh consent for secondary use of data, limiting use



Data Retention

Retaining data for the period required



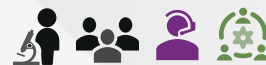
Data Classification

Assigning classification level to data



Data Storage & Transmission

Protecting data in storage & in-transit, managing access



Data Sharing

Third-party disclosure & monitoring



Data Disposal

Archiving or destroying data once no longer required



Possible Stakeholder Involvement



Office of Research Services
(including Research Facilitators)



Principal Investigators



Research Team Members
(including Student Researchers)



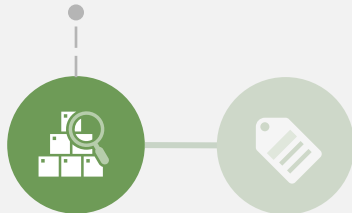
Technology Services
department (IT)

Data Identification | Roles & Responsibilities

PREPARATION



Data Identification



Data Classification



Principal Investigators

- ✓ Understand the **research data** collected and used and identify **sensitive and personal data**
- ✓ **Inventory the data** and how it flows throughout the information lifecycle
- ✓ **Identify the systems / applications** where the data exists and verify the ones that are University-provided or approved by IT



Research Team

provide guidance



IT Team

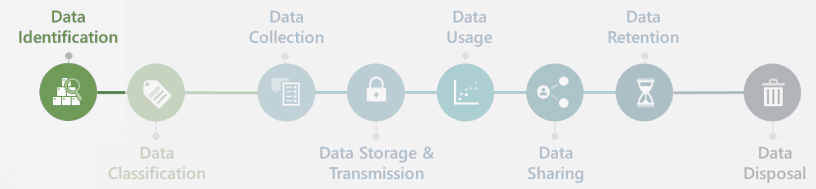
- ✓ Verify the **systems / applications** used in research activities that are **in-scope for IT's support** in implementing technical controls



Office of Research & Research Facilitators

- ✓ Provide **support and guidance** to Principal Investigators in determining the scope of how these guidelines apply to research data
- ✓ **Develop and maintain** the Guidelines & Standard and **make updates** as need.

Data Identification | Roles & Responsibilities



Principal Investigators & Research Team

Understand the data created, collected, and used for research activities and the sensitivity of the data

Do Lakehead's data classification guidelines apply to your research data?

 **In scope**

These guidelines apply to data that is **under your control**, where you are responsible for **collecting the data** and/or **responsible for storing and managing the data**.

 **Not in scope**

These guidelines do not apply to **data collected and managed by a third party** that you are **provided access to for use**.

Does your data involve sensitive, personal, or health information?



If yes – complete a **data inventory** to capture the information involved and **how it flows throughout** the research project information lifecycle.

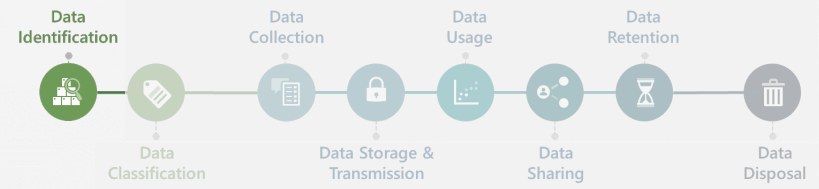
This will help you understand where to **implement data handling and protection controls** throughout the information lifecycle.

What technologies are involved? Are they University-provided or approved by IT?



- ✓ Identify all systems, applications, and devices where the data exists and **verify that they are University-provided or IT-approved**
- × Technologies that are **not University-provided or IT-approved** are not within the scope of the IT team's support. As such, you are responsible for **implementing the appropriate technical controls to protect data within these systems, applications, or devices**.

Data Identification | Roles & Responsibilities



Principal Investigators & Research Team

Understand the data created, collected, and used for research activities and the sensitivity of the data

Do Lakehead’s data classification guidelines apply to your research data?

In scope

These guidelines apply to data that is under your control, where you are responsible for collecting the data and/or responsible for storing and managing the data.

Not in scope

These guidelines do not apply to data collected and managed by a third party that you are provided access to for use.

Does your data involve sensitive, personal, or health information?



If yes – complete a data inventory to capture the information involved and how it flows throughout the research project information lifecycle.

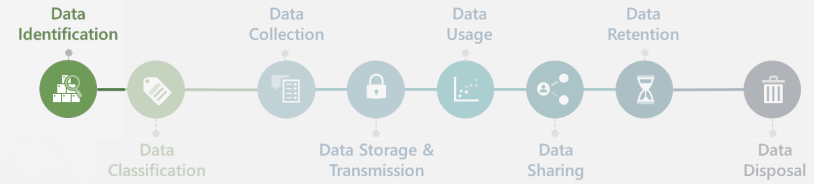
This will help you understand where to implement data handling and protection controls throughout the information lifecycle.

What technologies are involved? Are they University-provided or approved by IT?



- ✓ Identify all systems, applications, and devices where the data exists and verify that they are University-provided or IT-approved
- × Technologies that are not University-provided or IT-approved are not within the scope of the IT team’s support. As such, you are responsible for implementing the appropriate technical controls to protect data within these systems, applications, or devices.

Data Identification | Roles & Responsibilities



Principal Investigators & Research Team

Understand the data created, collected, and used for research activities and the sensitivity of the data

Do Lakehead's data classification guidelines apply to your research data?

 **In scope**

These guidelines apply to data that is **under your control**, where you are responsible for **collecting the data** and/or **responsible for storing and managing the data**.

 **Not in scope**

These guidelines do not apply to **data collected and managed by a third party** that you are **provided access to for use**.

Does your data involve sensitive, personal, or health information?



If yes – complete a data inventory to capture the information involved and **how it flows throughout** the research project **information lifecycle**.

This will help you understand **where to implement data handling and protection controls** throughout the information lifecycle.

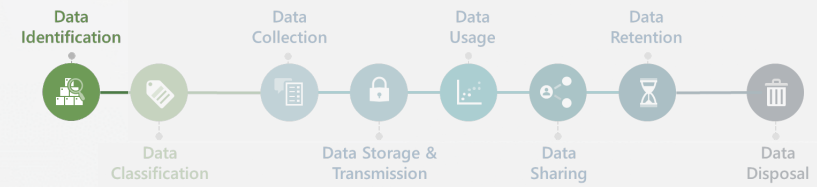
What technologies are involved? Are they University-provided or approved by IT?



- ✓ **Identify all systems, applications, and devices** where the data exists and **verify that they are University-provided or IT-approved**
- × **Technologies that are not University-provided or IT-approved are not within the scope of the IT team's support**. As such, **you are responsible for implementing the appropriate technical controls to protect data within these systems, applications, or devices**.

Test Your Knowledge

Data Identification In Action | Scenario A



A Principal Investigator's research project involves assessing the impacts of a cognitive disorder on diagnosed individuals' quality of life.

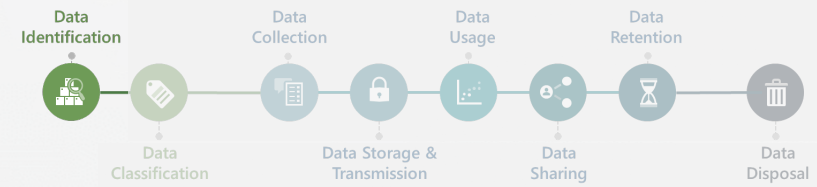
Through a partnership with a hospital in Ontario and with research participants' informed consent, the Principal Investigator accesses a subset of research participants' health information through the hospital's database.

? Do Lakehead's data classification guidelines apply to this research data?

A – Yes, these guidelines apply

B – No, these guidelines do not apply

Data Identification In Action | Scenario A



A Principal Investigator's research project involves assessing the impacts of a cognitive disorder on diagnosed individuals' quality of life.

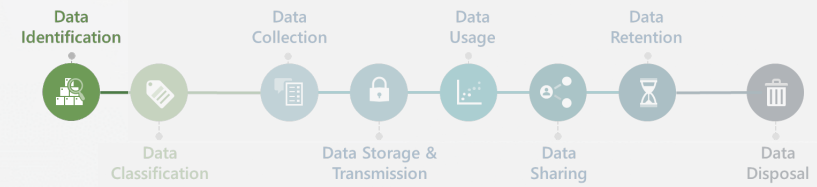
Through a partnership with a hospital in Ontario and with research participants' informed consent, the Principal Investigator accesses a subset of research participants' health information through the hospital's database.

? Do Lakehead's data classification guidelines apply to this research data?

- ✗ A – Yes, these guidelines apply
- ✓ B – No, these guidelines do not apply

Lakehead's guidelines do not apply here, as the data is collected and managed by the hospital and stored in their database; the research data is not under the control of the Principal Investigator, or within the University's environment.

Data Identification In Action | Scenario B



A Principal Investigator is developing intellectual property (IP) as part of their research project. The Research Project Team conducts analysis and collaborates on project documents through a shared Google Drive using their Lakehead University accounts.

The Principal Investigator also stores research data on their personal USB drive for ease of access while traveling remotely.



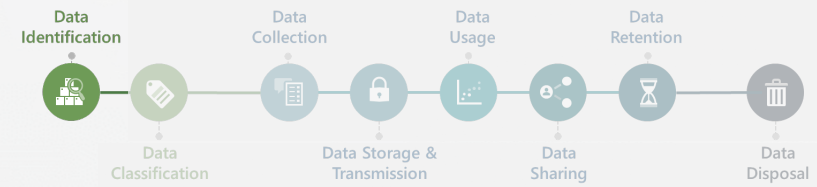
Who is responsible for implementing technical controls for safeguarding this research data?

A – IT team

B – the Principal Investigator

C – Both

Data Identification In Action | Scenario B



A Principal Investigator is developing intellectual property (IP) as part of their research project. The Research Project Team conducts analysis and collaborates on project documents through a shared Google Drive using their Lakehead University accounts.

The Principal Investigator also stores research data on their personal USB drive for ease of access while traveling remotely.

? Who is responsible for implementing technical controls for safeguarding this research data?

- ✗ A – IT team
- ✗ B – the Principal Investigator
- ✓ C – Both

Research data stored on the shared Google Drive → IT Team's responsibility, as this is within the University's environment

Research data stored on the Principal Investigator's personal USB drive → the Principal Investigator's responsibility, as this is not a University-provided or IT-approved device.

Data Classification | Roles & Responsibilities

PREPARATION



Principal Investigators

- ✓ Assign a **classification level** to all research data
- ✓ Identify the **appropriate controls** for handling and protecting research data based on the classification assigned

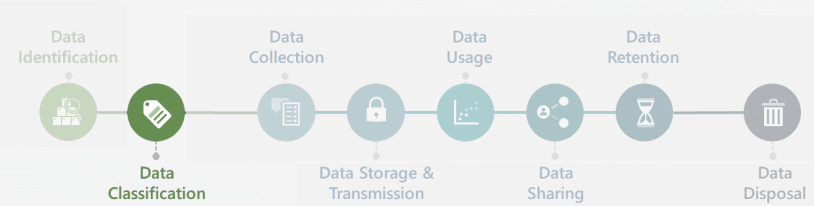


Research Team Members

- ✓ Understand the **classification level** assigned to research data being handled
- ✓ Apply the **appropriate controls** for handling and protecting research data based on the classification assigned


provide guidance

Data Classification | Roles & Responsibilities



Principal Investigators

Now that you have an understanding of the data involved in your research activities –

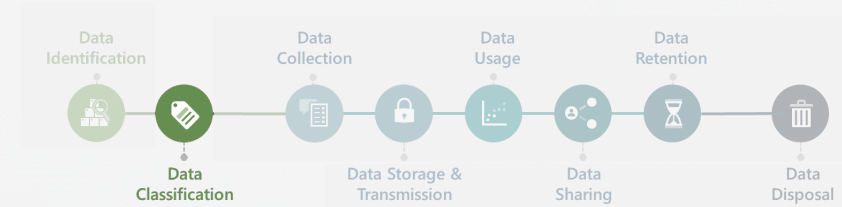
Assign a classification level to all research data. This will help you determine the appropriate controls for handling and protecting the data based on its sensitivity.

Confidential / Sensitive	Internal / Private	Public
Data only available to limited authorized individuals; unauthorized disclosure could result in severe harm to an individual or the University.	Data available to authorized users for research purposes; unauthorized disclosure could result in minor harm to an individual or the University.	Data that is deemed public by legislation or through a University policy; disclosure would not result in any harm to an individual or the University.
<ul style="list-style-type: none"> ❖ Human participants' name, address, health & medical information, income ❖ Intellectual property ❖ Unpublished research data & library transactions 	<ul style="list-style-type: none"> ❖ Research team meeting minutes & correspondence ❖ Contracts between researchers & community partners ❖ Project funders' contact information 	<ul style="list-style-type: none"> ❖ Published research data ❖ Researchers' name and business contact information ❖ Aggregated human subject data (where re-identification is not possible)



When assigning a classification level, **consider the legal obligations to protect the confidentiality** of the information, as well as the **risk of harm that may result** from the information's **unauthorized access, manipulation, or inadvertent disclosure.**

Data Classification | Roles & Responsibilities



Research Team

Understand the classification level assigned to research data and apply the appropriate controls for handling and protecting the data based on the classification assigned

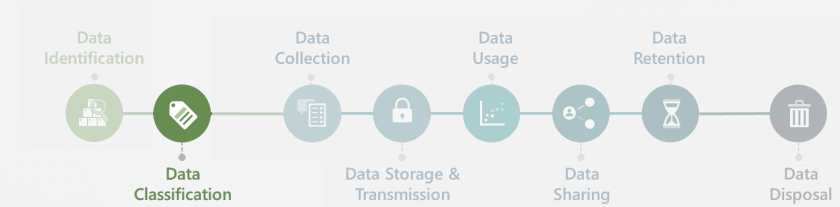
For all research data you are handling – ensure that you understand the classification level assigned to the data.

Based on the Principal Investigator's guidance, apply the appropriate controls for handling and protecting research data based on the classification assigned.



Refer to the full [Research Data Guidelines and Classification Standard](#) (available through the [Research & Innovation webpage](#)) for detailed guidance on the appropriate controls to be implemented for each classification level.

Data Classification In Action



Which classification level would you assign to the following research data elements?

Confidential / Sensitive

Data only available to limited authorized individuals; unauthorized disclosure could result in severe harm to an individual or the University.

Internal / Private

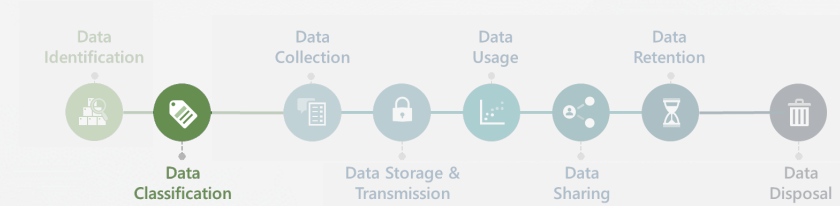
Data available to authorized users for research purposes; unauthorized disclosure could result in minor harm to an individual or the University.

Public

Data that is deemed public by legislation or through a University policy; disclosure would not result in any harm to an individual or the University.

Data Elements	Classification Level
1. Principal Investigator's business contact information	?
2. Research participant's education level	?
3. Meeting notes from a Research Team meeting discussing approach to conducting interviews with research participants	?
4. Working documents supporting the development of a patent	?

Data Classification In Action



Which classification level would you assign to the following research data elements?

Confidential / Sensitive

Data only available to limited authorized individuals; unauthorized disclosure could result in severe harm to an individual or the University.

Internal / Private

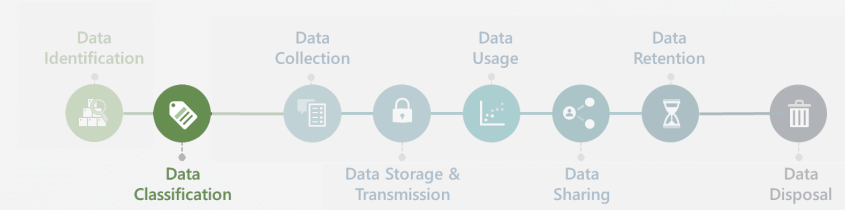
Data available to authorized users for research purposes; unauthorized disclosure could result in minor harm to an individual or the University.

Public

Data that is deemed public by legislation or through a University policy; disclosure would not result in any harm to an individual or the University.

Data Elements	Classification Level
1. Principal Investigator's business contact information	Public
2. Research participant's education level	?
3. Meeting notes from a Research Team meeting discussing approach to conducting interviews with research participants	?
4. Working documents supporting the development of a patent	?

Data Classification In Action

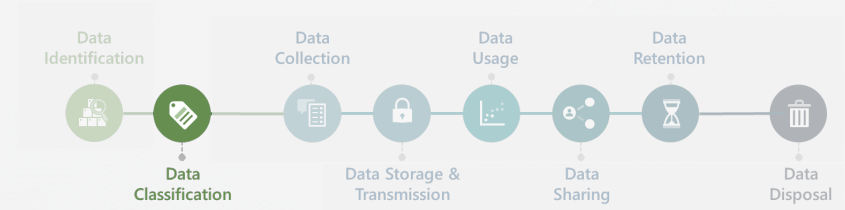


Which classification level would you assign to the following research data elements?

Confidential / Sensitive	Internal / Private	Public
Data only available to limited authorized individuals; unauthorized disclosure could result in severe harm to an individual or the University.	Data available to authorized users for research purposes; unauthorized disclosure could result in minor harm to an individual or the University.	Data that is deemed public by legislation or through a University policy; disclosure would not result in any harm to an individual or the University.

Data Elements	Classification Level
1. Principal Investigator's business contact information	Public
2. Research participant's education level	Confidential / Sensitive
3. Meeting notes from a Research Team meeting discussing approach to conducting interviews with research participants	?
4. Working documents supporting the development of a patent	?

Data Classification In Action

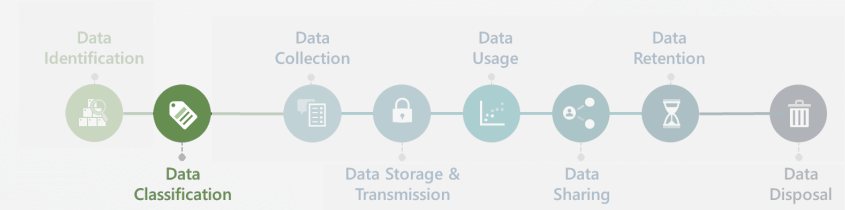


Which classification level would you assign to the following research data elements?

Confidential / Sensitive	Internal / Private	Public
Data only available to limited authorized individuals; unauthorized disclosure could result in severe harm to an individual or the University.	Data available to authorized users for research purposes; unauthorized disclosure could result in minor harm to an individual or the University.	Data that is deemed public by legislation or through a University policy; disclosure would not result in any harm to an individual or the University.

Data Elements	Classification Level
1. Principal Investigator's business contact information	Public
2. Research participant's education level	Confidential / Sensitive
3. Meeting notes from a Research Team meeting discussing approach to conducting interviews with research participants	Internal / Private
4. Working documents supporting the development of a patent	?

Data Classification In Action



Which classification level would you assign to the following research data elements?

Confidential / Sensitive	Internal / Private	Public
Data only available to limited authorized individuals; unauthorized disclosure could result in severe harm to an individual or the University.	Data available to authorized users for research purposes; unauthorized disclosure could result in minor harm to an individual or the University.	Data that is deemed public by legislation or through a University policy; disclosure would not result in any harm to an individual or the University.

Data Elements	Classification Level
1. Principal Investigator's business contact information	Public
2. Research participant's education level	Confidential / Sensitive
3. Meeting notes from a Research Team meeting discussing approach to conducting interviews with research participants	Internal / Private
4. Working documents supporting the development of a patent	Confidential / Sensitive

Data Collection | Roles & Responsibilities

PROJECT DURATION



Data
Collection



Data Storage &
Transmission



Principal Investigators



Research Team



Obtain consent from research participants

- ✓ Obtain **voluntary and informed consent** from research participants **before or at the time of data collection in accordance with TCPS 2 (2022)**.
- ✓ **Consent to participate in research should be obtained even if the data being collected does not contain personal information.**



Limit collection of sensitive and personal data

- ✓ **Limit the collection** of sensitive and personal information **only to what is necessary** and for the **purposes identified** at the time that consent was provided.



*provide
guidance*

Data Storage & Transmission | Roles & Responsibilities

PROJECT DURATION



Data Storage & Transmission



Principal Investigators

- ✓ Manage access to research data, including access provisioning, revocation, and monitoring
- ✓ Implement (and/or delegate the implementation of) controls to protect research data in-storage and in-transit



Research Team Members

- ✓ Support the Principal Investigator in implementing controls to safeguard research data in-storage and in-transit



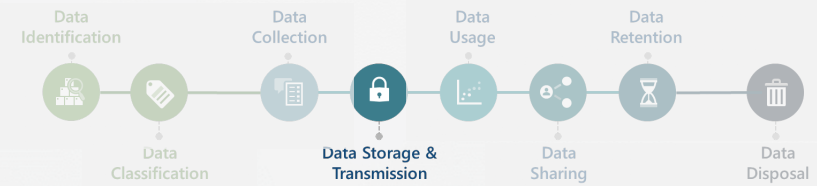
IT Team

- ✓ Implement technical security controls to safeguard data in-storage and in-transit
- ✓ Enable and retain audit logs of access to data and conduct threat and vulnerability management.



provide guidance

Data Storage & Transmission | Roles & Responsibilities



Principal Investigators

Manage access to research data, including access provisioning, revocation, and monitoring



Access should be provisioned based on roles on the research team and on a **need-to-know** basis – grant access to research data **only to those who require access** to fulfil their responsibilities.



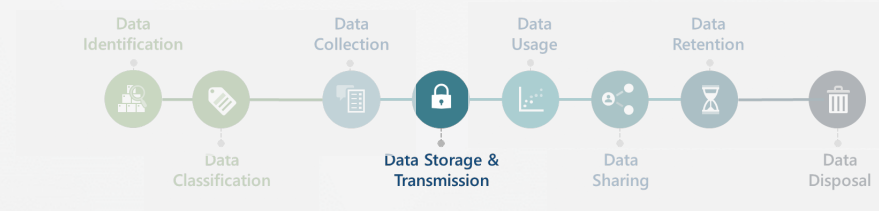
Prohibit copying, moving, and downloading of **'Confidential'** research data onto **local drives** and **removable media** (e.g., USB), unless explicitly authorized by the Principal Investigator for a defined purpose.



Regularly review the list of team members who have **access to 'Confidential' data** and **remove access if it is no longer required.**

Ensure all devices provided for research (e.g., USBs) are **returned by the team member.**

Data Storage & Transmission | Roles & Responsibilities



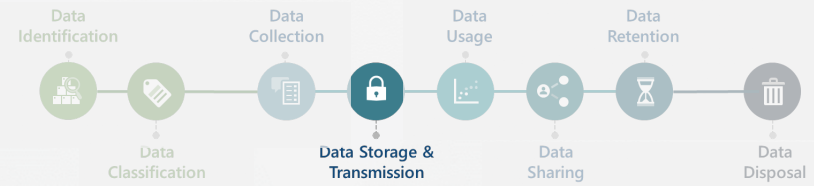
Principal Investigators

Implement (and/or delegate the implementation of) controls to protect research data at rest and in transit.

'Data at rest' is stationary data that is stored in an electronic or physical storage location.

'Data in transit' is data that is being transferred between electronic or physical locations.

Data Storage & Transmission | Roles & Responsibilities




Principal Investigators & Research Team


Implement (and/or delegate the implementation of) controls to protect research data at rest and in transit.

Protecting data at rest


Electronic data


 Storage of **'Confidential'** research data should be **restricted to University-provided technologies** (e.g., laptops, devices, and authorized applications).

'Confidential' research data **stored on personal devices** should be protected with mechanisms such as **password protection** and **antivirus software** if encryption is not possible.

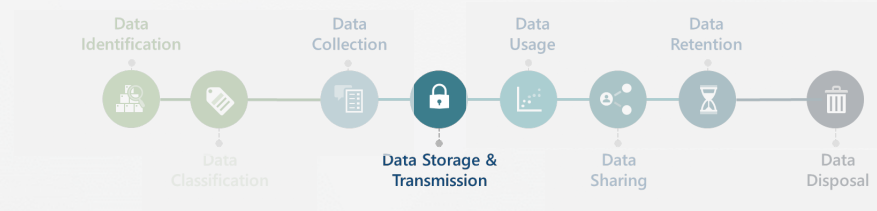
 In cases of exception where **removal media** (e.g., USB) is used to store **'Confidential'** research data, **engage IT** to ensure it is **encrypted** and **password-protected** prior to use.

Paper / hardcopy data

 **Research data** that is **not 'Public'** should **not be** left in **plain view** unattended.

 **'Confidential'** research data should always be **stored** in a **locked container** with the key accessible only by the Principal Investigator unless otherwise approved and authorized.

Data Storage & Transmission | Roles & Responsibilities



 **Principal Investigators & Research Team**  

Implement (and/or delegate the implementation of) controls to protect research data at rest and in transit.

Protecting data in transit

Electronic data



'**Confidential**' research data **should not be shared** through **email**. In cases of exception, these **emails should be encrypted** and **include the label 'Confidential'** in the email subject line.



Sharing of data should be done **only via secure** and **authorized means** that have been **approved by IT** (e.g., secure file transfer, secure portal). **Engage IT to confirm what is appropriate to use.**

Paper / hardcopy data



'**Confidential**' or '**Internal**' research data should be **labeled** when being moved (e.g., by post mail).



Use **sealed envelopes** or **tamper evident packaging**.

Data Usage | Roles & Responsibilities

PROJECT DURATION



Data Usage



Data Sharing



Principal Investigators



Research Team



Obtain fresh consent for secondary use of data

If a research participant's sensitive or personal information is being used for a new purpose (outside of the purposes they had originally consented to) –

- ✓ fresh consent must be obtained from the research participant **before** secondary use of their data.



Limit use of data to identified purposes

- ✓ Limit the use of sensitive and personal information **only to the purposes identified and consented to** by research participants before or at the time of collection.



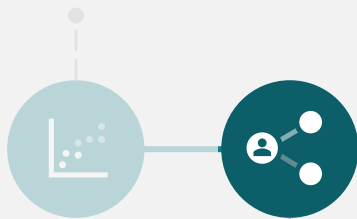
provide guidance

Data Sharing | Roles & Responsibilities

PROJECT DURATION



Data Usage



Data Sharing



Principal Investigators



Research Team



No 'Confidential' research data shall be disclosed to other research teams or departments at the University, or to 3rd parties, without the Principal Investigator and the research participant's express and informed consent.



Third parties' access to data should have in place:

- Data sharing agreement that documents controls aligned with Lakehead's guidelines
- Non-disclosure Agreement (NDA)
- Review and approval from the Principal Investigator



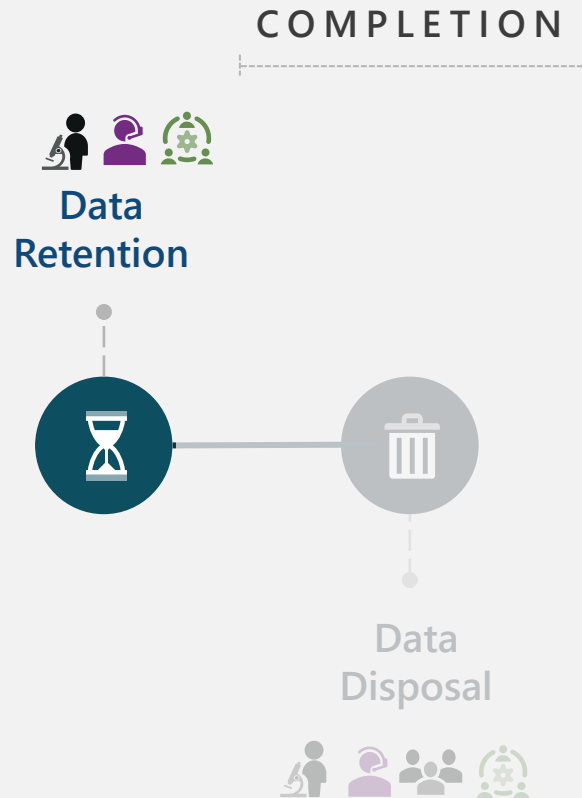
provide guidance

Office of Research & Research Facilitators



Maintain a **data sharing agreement template** for researchers that can be used when research data is shared with third parties.

Data Retention | Roles & Responsibilities



Principal Investigators



All research data, including 'Confidential' research data, is to be retained for a minimum of 7 years after the completion of research activities, as defined by the *LUFA Collective Agreement*.

If the research data is **subject to a separate retention schedule** based on specific contractual agreements, **retain the data based on the applicable retention requirements.**



Retaining Copy of Data Shared with Third Parties
For compliance purposes, when collaborating with and sharing data with external third parties, one copy of the data must be retained by the University for the minimum of 7 years or as otherwise required based on specific contractual agreements.



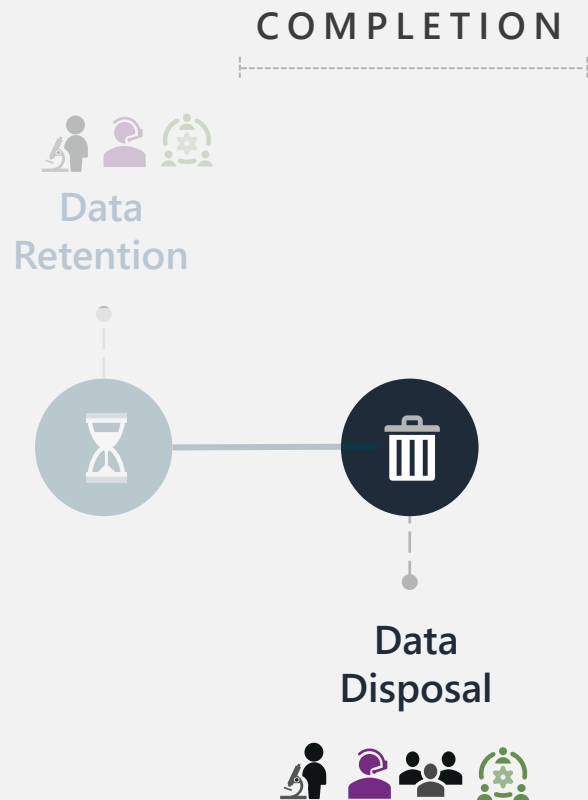
Research Team

IT Team






Implement the appropriate **data retention requirements** within in-scope systems / applications.

Data Disposal | Roles & Responsibilities




Principal Investigators


-  Ensure all devices provided for use during research activities (e.g., laptops, USBs) are returned by all research team members upon project completion.
-  Ensure that all research data is securely disposed of through the appropriate means (destruction or archival) in accordance with the applicable data retention requirements.
-  For data that is up for destruction or archival (i.e., the retention period has elapsed), **provide documented final approval to the delegated authority** (e.g., IT, third-party) **before** the data destruction or archival is carried out.

 *provide guidance*

Research Team

-  Return all devices provided for use during research activities to the Principal Investigator **upon project completion**.

IT Team

-  Implement the appropriate data destruction or archival requirements.

Data Disposal | Roles & Responsibilities

Principal Investigators

Ensure that all research data is securely disposed of through the appropriate means (destruction or archival) in accordance with the applicable data retention requirements.



For data that is up for destruction or archival (i.e., the retention period has elapsed), **provide documented final approval to the delegated authority** before the data destruction or archival is carried out.



Identify all the systems / applications where the data exists (as per the data inventory) to **ensure that all applicable data is destroyed or archived.**

Data Destruction Methods

Hardcopy data: Shred data and obtain a certificate of destruction if it is outsourced to a third party.

Electronic data: Destroy data, including backups, using a process that ensures the data cannot be recovered and used for unauthorized purposes.

Physical devices: Return University-provided devices to the Facilities team for secure destruction. Engage IT for guidance and support with return of physical devices if needed.

Third parties: At the end of a 3rd party contract, the service provider should return data to the University unless the University requests that the data be destroyed by the 3rd party. Completion of destruction should be certified in writing within a 30-day period.

Data Disposal | Roles & Responsibilities

Principal Investigators

Ensure that all research data is securely disposed of through the appropriate means (destruction or archival) in accordance with the applicable data retention requirements.



For data that is up for destruction or archival (i.e., the retention period has elapsed), **provide documented final approval to the delegated authority** before the data destruction or archival is carried out.



Identify all the systems / applications where the data exists (as per the data inventory) to **ensure that all applicable data is destroyed or archived.**

Data Destruction Methods

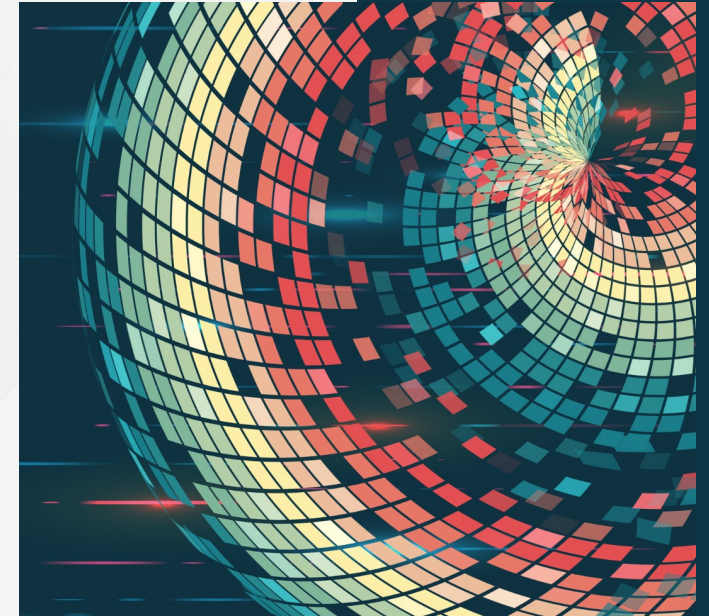
Hardcopy data: Shred data and **obtain a certificate of destruction** if it is outsourced to a third party.

Electronic data: Destroy data, including backups, using a process that **ensures the data cannot be recovered** and used for unauthorized purposes.

Physical devices: Return University-provided devices to the **Facilities team** for secure disposal. **Engage IT for guidance and support** with return of physical devices if needed.

Third parties: At the end of a 3rd party contract, the **service provider should return data** to the University unless the University requests that the data be destroyed by the 3rd party. Completion of destruction should be certified in writing within a 30-day period.

Training & Awareness Resources & Contact Information



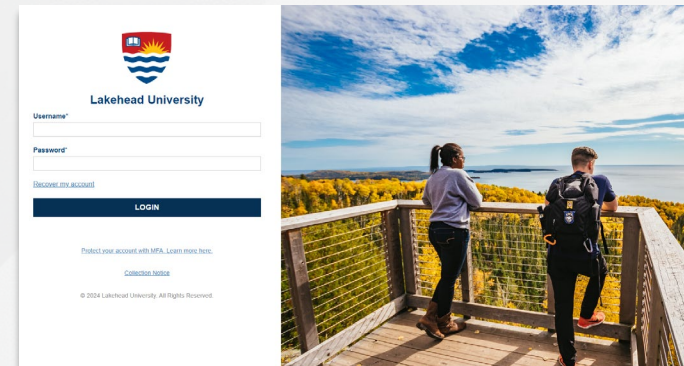
Data Classification Training & Awareness Resources

Access the full [Research Data Guidelines and Classification Standard](#) and [Data Classification Cheat Sheets](#) through the [Research & Innovation webpage](#)

Research & Innovation > Research Services > Resources

Data Classification Training Module

The online training module will be accessible through the [D2L platform](#)



Accessing Training Materials

(Research Data Guidelines and Classification Standard and Data Classification Cheat Sheets)

The screenshot shows the 'Research & Innovation' website. The header includes 'Home > Policies & Procedures'. A navigation menu on the left lists various categories, with 'Policies & Procedures' highlighted with an orange box. The main content area is titled 'Policies & Procedures' and lists numerous links related to research and innovation policies, such as 'Animal Emergency Response Plan', 'Biosafety Policy', and 'IPED Office Standard Operating Procedures - Full Version'.

The screenshot shows the 'Research & Innovation' website. The header includes 'Home > Research Services' and 'Set Campus'. A navigation menu on the left lists various categories, with 'Research Services' highlighted with an orange box. The main content area is titled 'Research Services' and provides information about funding and research opportunities. A 'Resources' section on the right is also highlighted with an orange box and lists links such as 'Grant-writing and Research Administration Resources' and 'Research and Innovation Services Information Guide For New Faculty'.

Support Contact Information



Office of Research Services

For questions and support on data classification and access to the data sharing agreement template, **connect with the Office of Research** by contacting Research@lakeheadu.ca



IT Team

For questions and support with implementing technical controls within University-provided or IT-approved technologies, **connect with the IT Team** by contacting HelpDesk@lakeheadu.ca

Data Classification Cheat Sheet – Researchers


DATA CLASSIFICATION *Cheat Sheet*

What is data classification?

Who does this apply to?

Assigning a sensitivity level to research data to identify and implement the appropriate controls for handling and protecting data based on sensitivity.

Anyone responsible for collecting, classifying, handling, sharing, or protecting research data at the University. This can include Principal Investigators, Research Facilitators, Graduate Students, Office of Research (ORS), and Technology Services (IT).



Research Data Classification Levels

	Confidential / Sensitive	Internal / Private	Public
Definition	Data only available to limited authorized users ; unauthorized disclosure could result in severe harm to an individual or the University.	Data available to authorized users for research purposes; unauthorized disclosure could result in minor harm to an individual or the University.	Data deemed public by legislation or through a University policy; disclosure would not result in any harm to an individual or the University.
Examples	<ul style="list-style-type: none"> ❖ Human participants' name, address, health & medical information, income ❖ Intellectual property ❖ Unpublished research data & library transactions 	<ul style="list-style-type: none"> ❖ Research team meeting minutes & correspondence ❖ Contracts between researchers & community partners ❖ Project funders' contact information 	<ul style="list-style-type: none"> ❖ Published research data ❖ Researchers' name and business contact information ❖ Aggregated human subject data (where re-identification is not possible)

Principal Investigator (PI) & Research Team (RT) Responsibilities

Data Identification	<ul style="list-style-type: none"> ✓ Understand research data collected and used and identify sensitivity of data ✓ Inventory sensitive data and its flow through the information lifecycle ✓ Identify technologies involved and verify the ones within scope of the IT Team's support (University-provided or IT-approved technologies)
Data Classification	<ul style="list-style-type: none"> ✓ PI: Assign a classification level to all research data and identify the appropriate controls for handling and protecting research data based on the classification assigned ✓ RT: Understand the classification level assigned and apply the appropriate controls for handling and protecting the data based on the classification
Data Collection	<ul style="list-style-type: none"> ✓ Obtain voluntary and informed consent from research participants before or at the time of data collection. ✓ Limit collection of data only to what is necessary and to the identified purposes
Data Storage & Transmission	<ul style="list-style-type: none"> ✓ Manage and limit access to research data on a role-based and need-to-know basis ✓ Implement controls to protect data in-storage and in-transit based on sensitivity ✓ Confidential data should not be shared through email; in cases of exception, removable media should be encrypted, and password protected before use
Data Usage	<ul style="list-style-type: none"> ✓ Obtain fresh consent for secondary use of data ✓ Limit use of data only to identified purposes at the time consent was provided
Data Sharing	<ul style="list-style-type: none"> ✓ Obtain consent from research participants before disclosing 'Confidential' data and ensure data sharing agreement is in place before disclosure to 3rd parties
Data Retention	<ul style="list-style-type: none"> ✓ Retain all research data for a minimum of 7 years after the completion of research activities, as defined by the LUFA Collective Agreement, or based on separate retention requirements the data may be subject to
Data Disposal	<ul style="list-style-type: none"> ✓ Ensure all research data is securely disposed of through destruction or archival in accordance with the applicable disposal requirements – return University devices to Facilities for secure disposal; engage IT for guidance if needed



Any questions for us?

