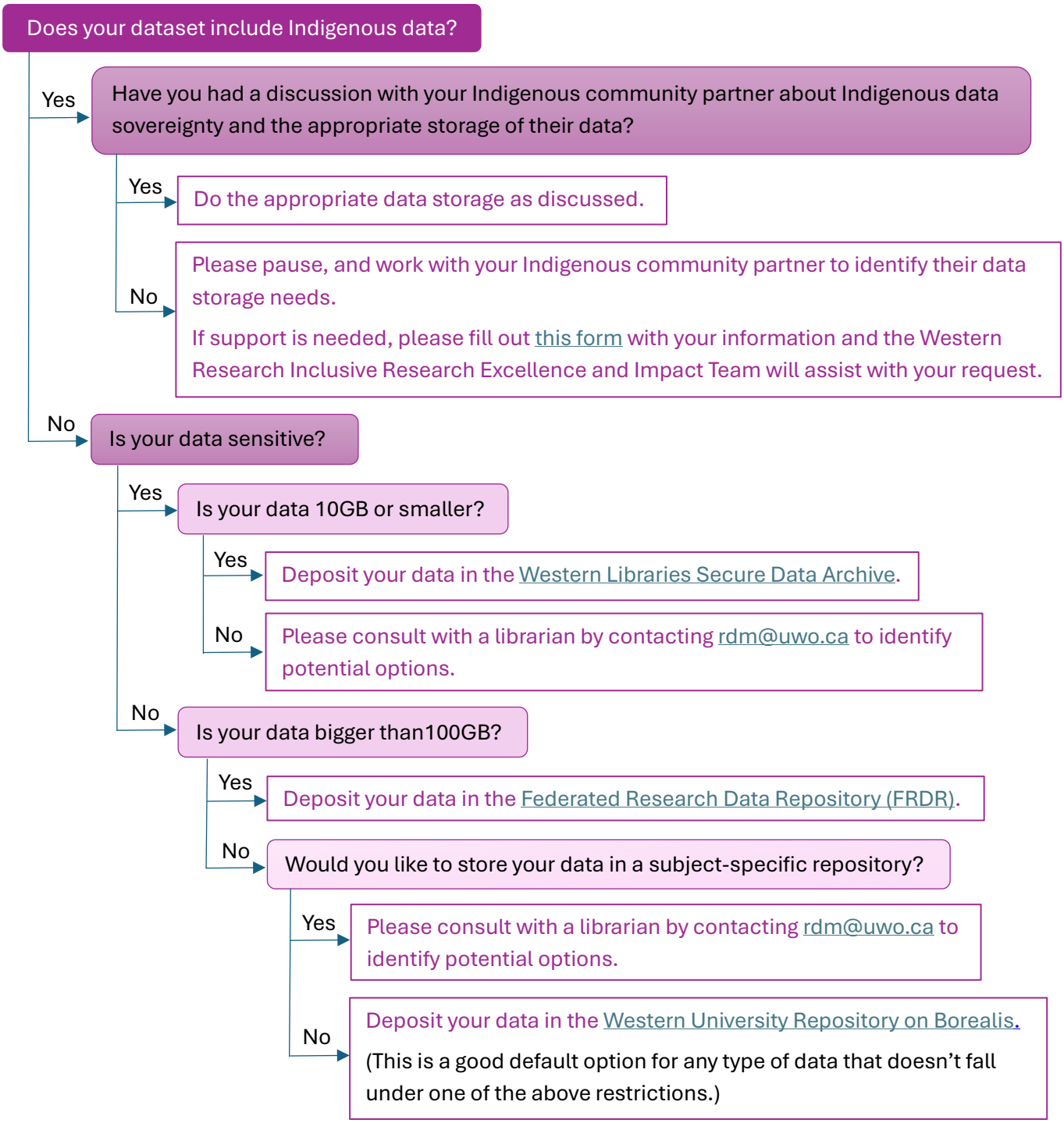
Data Repository Guidelines and Help Sheet

(Please see Glossary for definition of key terms, including: Data Repository, Open Data Repository, Secure Data Repository, Indigenous Data, and Sensitive Data.)



Glossary

- Data Repository: A data repository is a trusted storage space designed and managed to allow for long-term retention and management of research datasets and metadata describing those datasets. Data repositories can have varying requirements about what types of data they accept.

  Open Data Repository: An open data repository is a repository designed to allow both data sharing and long-term data retention. Open repositories may have limited access controls but do not have the security features required to protect sensitive data. An example of an open data repository is the Western Data Repository on Borealis.

  Secure Data Repository: A secure data repository uses controlled access management and other secure features to minimize the possibility of privacy breaches or other unauthorized access. Data in a secure data repository can only be accessed by active intervention on the part of the repository manager. An example of a secure data repository is the Western Libraries Secure Data Archive.

- Indigenous Data: Indigenous data is defined as "information and knowledge about individuals, groups, organizations, ways of knowing and living, languages, cultures, land, and natural resources. It exists in many formats, including Traditional Knowledge, which is defined as information that is passed down between generations. Traditional knowledge includes languages, stories, ceremonies, dance, song, arts, hunting, trapping, gathering, food and medicine preparation and storage, spirituality, beliefs, and world views. Indigenous data also include born-digital and digitized data collected by researchers, governments, and nongovernmental institutions."

- Sensitive Data: Sensitive data includes any data on people where research participants were promised confidentiality, where data cannot be shared without potentially breaking the law, or where data sharing may violate the trust of or risk harm to an individual, entity, or community.