# Guideline – What research data to store where

## 1. Purpose

This guide outlines best practice recommendations on how to classify, capture and store research data at AUT.

## 2. Scope

This guideline covers all staff, students, adjuncts and associates, and all research data. This guideline does not apply to administrative data, but both guidelines use the same data classification scheme. See the Administrative Data What to store where guideline.

## 3. How should I handle my research data

In relation to the planning of research data handling and it's actual processing and storage:

- Researchers should be familiar with the University Research Office's Data Management Tuia page and with AUTECs guidelines and procedures chapter 18 *The storage of data and consent forms*. A data management plan should be in place for all research data – and is required for Sensitive research data, or when data is being shared
- The handling and storage of research data must comply with the Privacy Act 2020
- The handling and storage of research data must take into consideration social and cultural requirements, for example, requirements around Māori Data Sovereignty
- Research data must be used and stored in accordance with the consent given by research participants
- A risk management approach must be used. When classifying data, the sensitivity should reflect the consequences of a breach on participants, the researchers, and AUT. The classification should always reflect the most sensitive data involved.
- Controls specified by data providers, ethics approvals and contractual agreements must be implemented
- Data and Consents are to be stored separately, this should be implemented as soon as is reasonably possible in the active phase
- It is the responsibility of researchers to ensure that Consents are treated with the utmost confidentiality

### 3.1 Lifecycle

There are multiple stages in the research data lifecycle. For this guideline, the lifecycle of research data is categorised into two broad phases:

- Active: this is the phase in which you are collecting, modifying, analysing data and reporting
- Post-analysis retention: this is the phase in which you have completed the above activities and are storing the data for the specified retention period. AUT's default position is that in this phase data is to be stored on AUT premises

## 3.2 Sensitivity Classification and Supported Platforms

| Classification | Description | Examples | Risk Consequence Category | Active Storage | Post-analysis retention Storage | Notes |
|---|---|---|---|---|---|---|
| **Public** | Files intended for an unrestricted or public audience | Open access or publicly available research data | Insignificant | SharePoint Online<br>OneDrive<br>Teams<br>Network Drives<br>REDCap<br>Qualtrics | SharePoint Online<br>OneDrive<br>Teams<br>Network Drives<br>Filling Cabinet<br>Iron Mountain | |
| **Private** | Files intended to be shared with a broad internal audience and/or limited external collaborators | Identifiable research data that has a low probability of discrimination, harm or unwanted attention resulting from disclosure | Minor | | | |
| | | Confidential research data | | | | |
| | | Re-identifiable/ de-identified research data | | | | |
| **Sensitive** | Files intended to be shared with a restricted internal audience and/or restricted internal collaborators | Identifiable research data that has a moderate probability of discrimination, harm or unwanted attention resulting from disclosure | Moderate<br>Major | | | |
| | | Re-identifiable/ de-identified health or medical data. Where personal data (including pseudonymised) emanates from the European Union, Special Categories of sensitive data are defined in Article 9 of the GDPR. | | | | |
| | | Audio Visual Recordings | | | | |
| **Very Sensitive** | Files intended to be shared with a highly restricted internal audience and/or highly restricted external collaborators | Identifiable health or medical or other data which has a high probability of discrimination, harm or unwanted attention resulting from disclosure | Major<br>Catastrophic | SharePoint Online<br>OneDrive<br>Teams<br>Network Drives<br>REDCap | SharePoint Online<br>OneDrive<br>Teams<br>Network Drives<br>Iron Mountain | If your data is subject to regulatory controls or is extremely sensitive (i.e. dual-use/military), Log a Job with ICT for Cybersecurity support |
| | | Identifiable data targeting specific ethnic groups, those with disabilities, or vulnerable groups | | | | |
| | | Audio Visual Recordings involving minors or other vulnerable people | | | | |
| | | Data subject to regulatory controls | | | | |

## 3.4. Notes

### Other cloud storage or processing platforms

Only use non-AUT managed cloud storage or processing platforms in collaboration with research partners whose institution manages the service. If you are unsure, ICT can advise you.

## 3.5 Summary

| | SharePoint Online | OneDrive | Teams | Network Drives | REDCap | Qualtrics | Filling Cabinet | Iron Mountain |
|---|---|---|---|---|---|---|---|---|
| **Sensitivity** | All levels | All levels | All levels | All levels | All levels | Up to and including Sensitive | All levels | All levels |
| **Stored in NZ** | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ |
| **Multi-Factor Authentication** | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | N/A | N/A |
| **Active Phase** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| **Archive Phase** | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ |