

Research Data Management and Data Protection Policy

Policy Owner	Head of Modelling and Simulation Unit
Approved By	ARNECH Scientific & Strategic Advisory Board
Effective Date	2021
Next Review Date	January 2027
Version	3.0
Applies To	All ARNECH staff, consultants, subcontractors, and field teams
Last Updated	January 2025

1. Purpose

This policy sets out how ARNECH collects, stores, manages, and protects research data, including health survey data, DHIS2 system data, and household-level information, throughout the research lifecycle.

2. Scope

This policy applies to all data collected, processed, or stored by ARNECH in the course of its research and consulting activities, and to all staff, consultants, and subcontractors with access to that data.

3. Policy Statement

ARNECH is committed to:

- Collecting only the data necessary for a defined research or evaluation purpose, with appropriate consent
- Storing data securely, with access restricted to authorised personnel on a need-to-know basis
- Anonymising or pseudonymising personally identifiable information wherever consistent with research objectives
- Retaining data only for as long as necessary, in line with client, donor, and statutory requirements, before secure deletion or archiving
- Complying with data-sharing agreements and cross-border data transfer requirements specified by clients, donors, and national regulators

4. Roles and Responsibilities

- The Head of the Modelling and Simulation Unit is responsible for data management standards and oversight of research databases.
- Project leads are responsible for ensuring their studies have an appropriate data management plan and secure data collection tools.
- All staff and consultants with data access are responsible for complying with this policy and any project-specific data-sharing agreement.

5. Procedures

- Each project maintains a data management plan covering collection tools, storage location, access controls, and retention and disposal schedule.
- Electronic data is stored on access-controlled systems with encryption in transit and at rest where feasible; paper records are stored securely and digitised promptly where possible.
- Data-sharing with clients, donors, or research partners follows a written data-sharing agreement specifying permitted use, security requirements, and retention terms.
- Personally identifiable information is separated from analytical datasets wherever possible, and access to identifying information is limited to staff with a defined need.

- Data breaches are reported to the Head of the Modelling and Simulation Unit immediately and assessed for notification obligations to affected individuals, clients, or regulators.

6. Reporting Concerns and Breaches

Suspected data breaches or misuse of data should be reported immediately to the Head of the Modelling and Simulation Unit or through the confidential whistleblowing channel, to enable rapid containment and, where required, notification to affected parties and regulators.

7. Training and Awareness

Staff and enumerators with data access receive briefing on secure data handling, consent procedures, and this policy prior to fieldwork, with periodic refreshers as tools or requirements change.

8. Related Standards and References

This policy is aligned with the following external standards and frameworks:

EU General Data Protection Regulation (GDPR) — <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

WHO Data Principles — <https://data.who.int/about/data/who-data-principles>

9. Monitoring and Review

This policy is reviewed by the Scientific & Strategic Advisory Board at least every two years, or sooner where changes in law, donor requirements, or organisational practice require it. Comments and proposed amendments may be submitted to the Policy Owner at any time.

Registration certificates, financial statements, and full policy documentation are available on request for prospective partners, clients, and funders as part of due diligence.

