

**Institute of Primate Research**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SOP No.** | **Issue Number** | **Issue Date** | **Revision Status** | **Revision Date** |
| **SOP/KIPRE/RPD/DSAS/3.1.76** | **Version 01** | **October 2025** | **-** | **-** |

**STANDARD OPERATING PROCEDURE (SOP) DOCUMENT**

**Data sharing, anonymisation, and compliance**

|  |  |  |  |
| --- | --- | --- | --- |
| **Approvals** |  |  |  |
|  | **Name** | **Signature** | **Date** |
| **Developed by:** | \_Patrick Waweru Mwaura\_ | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_6th October; 2025\_** |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **Reviewed by:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **Approved by:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

**Table of Contents**

[1. PURPOSE 4](#_Toc144316958)

[2. SCOPE 4](#_Toc144316959)

[3. PERSONS RESPONSIBLE: 4](#_Toc144316960)

[4. FREQUENCY 4](#_Toc144316961)

[5. MATERIALS 5](#_Toc144316962)

[6. PROCEDURE 5](#_Toc144316963)

[7. REFERENCES 6](#_Toc144316964)

# 

# PURPOSE

To establish standardized procedures for **data sharing, anonymisation, and compliance**, ensuring that all DS&AS-managed datasets are:

* **Protected and de-identified** according to ethical, legal, and institutional requirements.
* **Shared securely** with internal and external collaborators under controlled access.
* **Documented and auditable** to maintain transparency, reproducibility, and regulatory compliance.

This SOP aligns with:

**SOP 1** (Policies and Strategies), **SOP 2** (Regulatory Compliance), **SOP 6** (Data Access and Authentication), and **SOP 8** (Database and Workflow Management).

# SCOPE

Applies to all **DS&AS-managed datasets** that are shared **internally or externally**, including:

* Research collaborations and multi-institutional projects.
* Data supporting publications, reports, or dashboards.
* Deposits in open-access or institutional repositories.
* Activities requiring anonymisation, pseudonymisation, or aggregation before sharing.

# PERSONS RESPONSIBLE:

* **Head of DS&AS:** Reviews and authorizes all data-sharing requests to ensure compliance with institutional policies and strategic objectives.
* **Data Protection Officer (DPO):** Certifies that datasets comply with the **Kenya Data Protection Act (2019)**, GDPR, and institutional ethical standards.
* **Data Engineer / DS&AS Analyst:** Prepares datasets for sharing, applies anonymisation/pseudonymisation techniques, and implements **secure transfer mechanisms**.
* **Principal Investigator (PI):** Approves datasets for external sharing and ensures that all collaborators have signed **Data Use Agreements (DUAs)**.

# FREQUENCY

* **On-demand:** All data-sharing requests are processed as they arise, prior to any internal or external release.
* **Periodic audits:** Compliance with anonymisation, security, and regulatory requirements is reviewed **annually**.
* **Triggered reviews:** Additional audits are conducted following legal/regulatory changes or reported incidents involving data sharing.

# MATERIALS

* **Data Sharing Agreement (DSA) templates** – for formalizing data use terms with collaborators.
* **Secure transfer tools** – SFTP, VPN, HTTPS/SSL, or other institutional encrypted channels.
* **Anonymisation and pseudonymisation tools** – R/Python scripts, sdcMicro, ARX, or differential privacy tools.
* **Data dictionaries and metadata templates** – to accompany shared datasets for clarity and reproducibility.
* **Compliance checklists** – to verify legal, ethical, and institutional requirements before sharing.

# PROCEDURE

1. **Request Submission:**  
    • Collaborators submit a formal **Data Sharing Request** specifying dataset, purpose, and intended use.
2. **Pre-Review:**  
    • DS&AS verifies dataset availability, classification (Open, Restricted, Confidential), and internal readiness for sharing.
3. **Compliance Review:**  
    • DPO reviews request against **Kenya Data Protection Act (2019)**, GDPR, institutional policies, and ethical approvals.  
    • Any conditions for data use are documented.
4. **Anonymisation / Pseudonymisation:**  
    • DS&AS Analyst/Data Engineer applies appropriate de-identification techniques to protect sensitive fields.  
    • Metadata and data dictionaries are updated to accompany the shared dataset.
5. **Approval:**  
    • Head of DS&AS reviews anonymisation, compliance checks, and authorizes dataset release.  
    • PI confirms that all collaborators have signed **Data Use Agreements (DUAs)**.
6. **Secure Transfer:**  
    • Data is shared via **encrypted channels** (SFTP, VPN, HTTPS/SSL).  
    • All access and transfer events are logged in the DS&AS **Data Sharing Log**.
7. **Archiving:**  
    • Copies of shared datasets, approvals, anonymisation records, and DUAs are stored in the institutional repository with version control.
8. **Compliance Audit:**  
    • Annual audits are conducted to ensure that all shared datasets, procedures, and logs comply with legal, ethical, and institutional standards.  
    • Interim reviews triggered by incidents or regulatory updates.

# REFERENCES

1. Kenya Data Protection Act (2019) and amendments.
2. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).
3. KIPRE Institutional Data Protection and Sharing Policy (2024).
4. FAIR Data Principles (Wilkinson et al., 2016).
5. HIPAA – Health Insurance Portability and Accountability Act (1996).
6. ISO/IEC 27001:2022 – Information Security Management Systems.
7. DS&AS SOP 1 – Policies and Strategies.
8. DS&AS SOP 2 – Alignment with Institutional and National Regulations.
9. DS&AS SOP 6 – Data Access and Authentication Procedures.
10. DS&AS SOP 8 – Database and Workflow Management.

# ****APPENDICES****

**Appendix 9.1 – Forms and Templates**

1. **Data Sharing Request Form** – for collaborators to specify dataset and intended use.
2. **Data Use Agreement (DUA) Template** – formal agreement outlining terms of use, security, and compliance.
3. **Anonymisation / Pseudonymisation Checklist** – verifies all sensitive fields are appropriately de-identified.
4. **Data Sharing Log Template** – records dataset shared, recipients, approval dates, and transfer method.

**Appendix 9.2 – Tools and Systems**

* Anonymisation Tools: R packages (sdcMicro), Python scripts, ARX, differential privacy frameworks.
* Secure Transfer Tools: SFTP, VPN, HTTPS/SSL, encrypted cloud storage.
* Documentation Tools: Data dictionaries, metadata templates, workflow logs.
* Compliance Monitoring: DS&AS Data Sharing Dashboard and version-controlled repository.