GOVERNMENT OF KERALA

Kerala State Data Policy (Draft)

2026

Preamble

"In an era where data drives decision-making, innovation, and economic growth, the Government of Kerala recognizes the immense value of data in fostering transparency, accountability, and citizen empowerment. Data serves as a cornerstone for effective governance, enabling the seamless sharing of information to improve public services, enhance disaster management, stimulate research, drive industrial growth, and create new opportunities for economic development.

The State Data Policy of Kerala is founded on principles of openness, accessibility, and security, ensuring that data generated by government entities is harnessed responsibly for the benefit of society. By addressing challenges such as data silos and lack of standardization, and by aligning with national frameworks such as the National Data Sharing and Accessibility Policy (NDSAP), 2012 and integrating robust privacy safeguards, this policy emphasizes the importance of ethical and efficient data usage.

Through this initiative, Government of Kerala aims to establish an environment where data is utilized as a shared resource to enhance innovation, collaboration, and informed decision-making. The policy focuses on balancing data accessibility with privacy and security, setting the groundwork for a data-driven state where citizens have access to information, government operations are transparent, and the economy benefits.

2. Definitions

- **Data:** A representation of information, numerical compilations and observations, documents, facts, maps, images, charts, tables and figures, concepts in digital and/or analog form.
- **Real-Time Data:** refers to information that is obtained, processed, and presented immediately or with minimal delay as soon as it is generated.
- **Data Archive:** A place where machine-readable data are acquired, manipulated, documented, and distributed to others for further analysis and consumption.
- **Data Generation:** Initial generation / collection of data or subsequent addition of data to the same specification.

- **Data set:** A dataset is a structured collection of data organized and stored together for analysis or processing.
- **Geospatial Data:** All data which is geographically referenced
- **GIGW -** Guidelines for Indian Government Websites
- **Information:** Processed data
- **Metadata:** The information that describes the data source and the time, place, and conditions under which the data were created. Metadata informs the user of who, when, what, where, why, and how data were generated. It allows the data to be traced to a known origin and known quality.
- **Negative list:** Non-sharable data as declared by the departments / organizations. These datasets are considered non-shareable due to their sensitive nature and may include information that could compromise national security, violate individual privacy, breach legal or contractual obligations if disclosed.
- **Open Data:** It refers to data that is freely available for anyone to access, use without restrictions, typically provided in machine-readable formats.
- **Personal data:** means any data about an individual who is identifiable by or in relation to such data;
- **Sensitive personal data or information**: means such personal information which consists of
    - Password
    - Sex Life and Sexual Orientation
    - Biometric information
    - Information received by body corporate for processing, stored or processed under lawful contract or otherwise
    - Financial Data, including information related to financial information such as Bank account/credit card/debit card/payment instrument details of the users
    - Health Data, including physiological and mental health condition and medical records and history

    - Official identifier
    - Genetic Data
    - Transgender status/Intersex status
    - Caste or tribe
    - Religious or political belief or affiliation
- **Standards:** A set of established guidelines, protocols, or specifications that ensure data quality, interoperability, exchange, storage and reusability.
- **“Data Fiduciary”** means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
- **“Data Principal”** means the individual to whom the personal data relates and where such individual is— (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf.
- **“API”** - The term Application Programming Interface (API) means any mechanism that allows a system or service to access data or functionality provided by another system or service. The API is generally used to interact (like query, list, search, sometimes submit & update) directly with the specific information on a system, to trigger some action on other systems, or to perform some other action on other systems.

3. Objectives

- The Kerala State Data Policy (KSDP) will facilitate secured storage, access-controlled sharing and improved access to the data assets across all levels of Government.
- The policy shall be applicable to all types of data, whether electronic or in the form of physical records.
- The objectives of the policy are:
    - To define a set of guidelines relating to the classification of data within government, its ownership, and handling.
    - To define a set of guidelines and principles to help create an ecosystem for both open access to public data and controlled,

secure sharing of internal government data to relevant stakeholders protecting the rights of the information provider and the consumer.

- Facilitate the accessibility of authentic and shareable data and information to all the stakeholders through an integrated State Data Exchange platform thereby minimizing the extent of data collection by Govt. institutions.
- To integrate the State Data Exchange Platform with the Open Government Data (OGD) Platform of Government of India for the sharing of Open data.
- To promote the advanced data analytics capabilities and facilitate data driven decision making in policy formulation for the Government of Kerala.
- To facilitate extensive use of data in the implementation of Government programs and in disaster management situations in the state.
- To enforce the adoption of uniform data standards, metadata standards, and interoperability protocols, to ensure seamless data exchange, quality, and reusability across government departments and with external stakeholders.

4. Scope of the Policy

- Kerala State Data Policy (KSDP) will be applied to all the data created, generated, collected, stored or processed by any department, office, agency, or entity of the Government of Kerala (herein after referring to as Govt. institutions), either directly or through outsourced agencies, using public funds.
- This policy defines the specific levels and conditions of data access, covering both open and restricted categories.
- This Policy is applicable to data generated through electronic delivery of services by State departments, as well as to legacy data in both electronic and physical formats.

5. Benefits of the Policy

- This data policy facilitates the sharing of data among various State Departments through secure access control mechanisms.

- It ensures the completeness and accuracy of dataset descriptions, promotes adherence to data standards, and helps reduce costs, redundancy, and duplication of efforts
- It creates new opportunities for startups and research organizations by fostering innovation and driving economic growth through the use of open data.
- It facilitates data-driven decision-making by equipping policymakers with accurate, timely, and relevant information to inform effective governance.

6. Nodal Department

The Electronics & IT Department, Government of Kerala will be the nodal department for the implementation of this policy. Any subsequent modifications to this policy shall be governed by Electronics & IT Department.

7. Nodal Agency for implementation

Kerala State IT Mission (KSITM) is the nodal agency for the implementation and management of State Data Exchange Platform. KSITM will organize training programs to enhance the data management skills of government officials such as the designated Chief Data Officers (CDO), including data security, collection, storage, analysis etc.

The Director of the Kerala State IT Mission shall serve as the Chief Data Officer of the State, responsible for coordinating with the department-level CDOs to oversee the collective data management and publishing efforts across the State.

8. Technology Platform

- The sharing of data from various departments shall be done through a centrally integrated repository known as “State Data Exchange Platform”.
- The State Data Exchange Platform will facilitate secure data sharing among the Government institutions through user authentication and Role Based Access Control (RBAC) mechanisms.
- The State Data Exchange platform will be implemented and maintained by Kerala State IT Mission (KSITM) ensuring secure, seamless, and efficient data exchange between information providers

and consumers. The key functionalities proposed in the platform include:

- Data Exchange Setup & Configuration: Establishing a robust mechanism for data exchange across government departments and other stakeholders.
- Data Provider Onboarding: Identifying and integrating various data providers into the platform.
- Data Ingestion, Integration & Quality Reporting: Ensuring standardized data ingestion, integration and automated quality checks.
- User Interface (UI) Customization: Adapting the platform with custom branding and user-friendly interfaces, adopting the platform with GIGW compliance for accessibility.
- Access Management: Implement Access management to ensure secure data access to authorized users.
- Scalability & Performance Optimization: Enabling high availability, auto-scaling, and fault tolerance.
- Support & Maintenance: Ensuring long-term operational efficiency and security compliance.
- API Registry: Maintain an API repository within the State Data Exchange platform
- Security controls, logging, hashing and time-stamping, immutable audit trails, incident response, reporting, and related functions.

9. Data Classification

This policy aims to cover all types of data including geo spatial data generated by Government agencies/institutions using public funds in Kerala. Data generated or stored by the government agencies shall be classified as “Public”, “Internal” and “Confidential”.

a) **Public Data:** This category refers to data identified for proactive public dissemination, aligning with Open Data principles. It is generally made available with "Open Access" through the State Data Exchange platform and the Open Government Data (OGD) Platform of Government of India. This data should excludes personal data, sensitive personal information, or confidential data.

b) **Internal Data:** Data that is created, collected, processed, and stored by any State Government entity, department, or agency for its official use. This category refers to data that can be shared with other Government Departments / institutions for official purposes through the State Data Exchange platform on a "Restricted Access" basis.

c) **Confidential Data:** This refers to sensitive data that is protected from public disclosure due to its potential impact on national security, individual privacy, or cannot be publicly disclosed as per the applicable laws in India. These categories are subject to strict access controls and are sharable through the State Data Exchange mechanisms with explicit, highly controlled authorization processes that may be defined by the respective Department or Agency.

- Datasets shall be created preferably in machine readable formats only. Legacy data available in departments may also be identified and digitized in a phased and systematic manner, as appropriate.

- It shall be the responsibility of every Government Department, agency, or institution covered under this Policy to identify, assess, and categorize datasets generated, collected, or maintained by them into the prescribed categories of Public Data, Internal Data, or Confidential Data, in accordance with the guidelines issued under this Policy. Each Department shall ensure that such categorization is carried out in a transparent and consistent manner, and that datasets classified as Public or Internal Data are prepared for timely publication on the State Data Exchange Platform, unless specifically included in the approved Negative List. The Data Management Cell within each department or institution shall oversee and implement this process.

10. Types of Data Access

All Government institutions are obliged to grant access to and sharing of data assets generated by them using Government funds, based on any of the following access criteria in the State Data Exchange.

- **Open Access** without any authorization/registration applicable to the “Public Data” category.
- **Restricted Access** in which departments/organizations can access datasets through registration and prior authorization, applicable to the “Internal Data” category.

Approval Process

- The internal data published on the State Data Exchange platform by Government institutions shall be in accordance with the access controls defined by the State-level Data Governance Committee.
- The Chief Data Officer (CDO) of any State Government Departments can access and consume all datasets available to them on the platform without undergoing any additional approval process.
- The State Data Exchange will also provide a formal mechanism for requesting access to specific datasets that are not made available to users by Government institutions. Such requests shall be routed to, and approved by, the respective Departmental Chief Data Officers (CDOs) through this platform.

11. Negative List Preparation

- **Preparation of Negative List**
  - Each Department, through its **Departmental Data Management Cell (DMC)**, shall prepare a draft *Negative List* of datasets that cannot be shared due to reasons of national security, confidentiality, privacy, or statutory restrictions.
  - The draft list shall be prepared within six months from the date of notification of this Policy.
- **Approval Process**
  - The draft *Negative List* prepared by the DMC shall be submitted to the **State-level Data Governance Committee (SDGC)** for review.
  - The SDGC shall evaluate whether the inclusion of each dataset in the Negative List is consistent with:
    - The **Digital Personal Data Protection Act, 2023**,
    - The **Right to Information Act, 2005**,
    - The **National Data Sharing and Accessibility Policy (NDSAP), 2012**, and
    - Any other applicable State or Central legislation.
  - Upon recommendation by the SDGC, the list shall be forwarded to the **Apex-level Data Governance Committee** for final approval.
- The Negative List of datasets for departments shall be periodically reviewed by the State-level Data Governance Committee.

12. Apex-level Data Governance Committee

The Apex level Data Governance Committee will be a high-level decision-making body responsible for overseeing the administration of this policy and providing strategic directions. The Committee will be composed of the following members:

- Chief Secretary, Government of Kerala - Chairperson
- Additional Chief Secretary, Finance
- Additional Chief Secretary, Home & Vigilance
- Additional Chief Secretary, Revenue & Disaster Management
- Additional Chief Secretary, GAD
- Secretary, Law Department
- Additional Chief Secretary, Industries & Commerce
- Additional Chief Secretary, Health
- Secretary, Planning & Economic Affairs
- Secretary, E& IT Department (Convenor)
- Director, Kerala State IT Mission
- State Informatics Officer (SIO), NIC

- This committee would:
  - Administer the policy implementation, decides on the pricing or monetization measures to be taken with respect to data sharing.
  - Will be an appellate body to address any grievances from the Government Departments related to data sharing.
  - Recommend amendments to the policy from time to time.
  - The Apex-level Data Governance Committee shall have the authority to address disputes or non-compliance reported by the State-level Data Governance Committee (SDGC). It may issue necessary orders and directions to the concerned Government departments, agencies, or institutions to ensure adherence to the provisions of this Policy. It will act as an appellate body for any directions issued by SDGC regarding data sharing and publication.

13. State-level Data Governance Committee

The State level Data Governance Committee will be responsible for overseeing the implementation of this policy. The Committee comprises of the following members:

- Secretary, Electronics & IT Department (Chairperson)
- Representative from Finance Department
- Representative from Planning & Economic Affairs
- Director, Kerala State IT Mission (Convenor)
- State Informatics Officer (SIO), NIC
- Executive Director, CDAC
- Representative of the Departments concerned, attending as Special Invitee (Data Requestor and Data Owner)

This committee would:

- Responsible for implementing this policy in the State, reviewing the progress of data sharing by the Government institutions.
- Recommend any corrective measures to be taken with respect to inter-departmental data exchange.
- Define and approve access control mechanisms for datasets published on the State Data Exchange platform.
- Developing data standards and metadata guidelines, primarily by adopting and extending national standards and interoperability frameworks, monitoring data quality and compliance, addressing data-related issues and challenges.
- This Committee shall monitor compliance and facilitate coordination among departments to ensure timely data publication. In cases of non-compliance, the State-level Data Governance Committee shall have the operational authority to direct any Government Department, agency, or institution within the State to mandatorily publish datasets classified as Public Data or Internal Data on the State Data Exchange Platform within a specified timeframe.

- In case of unresolved disputes, the matter shall be escalated to the Apex-level Data Governance Committee, which serves as the appellate authority.

14. Data Management Cell in Departments (DMC)

Each Department would establish a Department Data Management Cell constituting members familiar with IT Systems of the Department. The Data Management Cell shall be headed by the Chief Data Officer (CDO).

The Data Management Cell would be responsible for:

- Prepare a schedule of departmental datasets to be released
- Prepare the Negative List for the Department, classify the datasets as per the policy.
- Identify the datasets and categorize them to publish in the State Data Exchange platform on a regular basis.
- Extend technical support for the preparation of datasets, conversion of formats etc.
- Monitoring and managing the open data within their respective Department, with a focus on data quality and accuracy.
- Institutionalize the creation and regular updating of datasets as part of routine operations, while ensuring data quality.
- Ensure data exchange mechanisms are effectively linked with broader government initiatives such as the Unified Services Delivery Portal (USDP) and the Unified Registry being implemented by Kerala State IT Mission, as relevant, to strengthen the delivery of integrated public services.
- Develop Open APIs for all the Departmental applications for enabling data exchange with other e-Governance applications or systems. The API shall be designed in accordance with the Indian Standard for Unified Data Exchange (IS 18003 (Part 2): 2021) and published in the API registry provided by the State Data Exchage platform.

Chief Data Officer

- The Head of the Department (HoD) or a senior officer is to be nominated as the Chief Data Officer (CDO) by each

Department/Organization. The details of the CDO shall be informed to Kerala State IT Mission.

- The responsibility of Chief Data Officer is as follows:
    - The Chief Data Officer (CDO) is responsible for comprehensive management, strategic use, and governance of data across their respective department/organization.
    - The Chief Data Officer (CDO) should publish the datasets from their Department or institution to the State Data Exchange platform.
    - The Chief Data Officer (CDO) shall submit requests via the State Data Exchange platform to access datasets from other Government institutions. All such requests will be evaluated by the State-level Data Governance Committee.
    - Oversee the management of organizational data across its entire lifecycle: collection, storage, processing, quality assurance, retention and archiving.
    - Lead the open data initiative of the department by coordinating with the Solution Provider / Application development Agency for the development of Application Programming Interface (API) for data sharing.

15. Personal Data Sharing and Protection

- **Compliance with DPDP**
    - Any sharing or processing of personal data shall strictly adhere to the provisions of the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Digital Personal Data Protection Rules, 2025, regulations, and guidelines issued thereunder.
    - All Government institutions that collect and process personal data shall be designated as Data Fiduciaries under the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025. They shall ensure that data sharing practices respect the rights of Data Principals, in accordance with the Act and its associated rules
- **Sharing of Personal Data Across Government Departments**

Personal data may be shared across Government Departments only when:

- It is necessary for delivering public services or performing statutory functions;
- Data minimization principles are applied (only required data is shared);
- Consent and/or lawful grounds for processing under DPDP Act 2023 and DPDP Rules 2025 are ensured.

- **Sharing with External Entities**

  No personal data shall be shared with external agencies, private entities, or third parties unless:

  - Explicit consent of the Data Principal is obtained, or;
  - Such sharing is mandated under law or approved by the competent authority under the DPDP Act.

- **Departmental Responsibility**

  - Each Department ensure compliance with the DPDP Act while sharing personal data, including implementing safeguards such as encryption, access control, consent management, and audit trails.
  - Departments must designate their Chief Data Officer (CDO), Data Protection Officer (if applicable as per DPDP Act, 2023) as responsible for monitoring and enforcing compliance in data sharing.
  - In accordance with the Digital Personal Data Protection Act, 2023, each Government department, agency, or institution covered under this Policy shall establish a transparent and time bound grievance redressal mechanism to address complaints related to personal data processing.

16. Data Storage, Retention and its Archival

All government entities shall comply with established best practices for data storage to ensure the security, integrity, and accessibility of data. These standards shall cover aspects such as the use of secure and scalable storage infrastructure, regular data backups, disaster recovery

mechanisms, encryption protocols, access controls, and compliance with relevant data protection laws.

- **Archival Policies:** "Each department, through its Data Management Cell (DMC), shall develop and implement comprehensive data archiving protocols or guidelines. These will define criteria for identifying data suitable for archiving, the format for archival (e.g., long-term preservation formats), and establish secure procedures for both storing and retrieving archived data.
- **Responsibility for Archival:** The Chief Data Officer (CDO) within each department will be responsible for overseeing the timely and secure archiving of relevant datasets.
- **Retention Schedules:** Departments shall establish clear data retention schedules for all categories of data. These schedules will specify the minimum and maximum retention periods based on legal, regulatory, and operational requirements. Retention schedules shall be periodically reviewed and updated by the respective DMCs to ensure ongoing compliance and relevance.

17. Pricing

- Inter-departmental sharing of datasets classified as Internal data on the State Data Exchange platform by the State Government institutions shall be free of cost, thereby enabling seamless data exchange across government sectors.
- Certain datasets classified as “Internal Data” on the State Data Exchange platform may be monetized by the Government institutions given the substantial investment involved in their collection, storage, and maintenance. The institution concerned submit a formal request for monetization, along with the proposed costing structure, to the Apex-level Data Governance Committee for approval.
- Only anonymized data could be shared and monetized. The Chief Data Officer (CDO) or designated Data Protection Officer shall ensure that any data shared for monetization excludes personal data of beneficiaries, as well as datasets classified under the Negative List or marked as Confidential. All such activities must comply with the personal data sharing and protection principles outlined in this Policy/

guidelines. Such pricing, however, shall apply only to private entities—including startups, industries, and other non-governmental stakeholders—and shall not be applicable to Government institutions.

- Monetization for datasets shall be restricted only to value-added datasets where substantial processing, enrichment, or curation has been carried out by the concerned Government institution. The principle of cost-recovery shall apply, and no profit-making shall be pursued. All basic Open Data shall remain free of cost and accessible to the public in accordance with Open Government Data principles.

18. Legal Framework

- Data ownership shall remain with the respective Government institutions that collected the data and act as the Data Fiduciaries under applicable law. The data shall reside within their IT-enabled infrastructure and be made available for sharing and access in accordance with prescribed governance and security protocols as per this policy.
- Chief Data Officers are responsible in understanding and applying the legal and ethical restrictions associated with data in their functional areas, as well as ensuring that proper procedures are implemented to meet these requirements.
- Any suspected unauthorized access to restricted and regulated data must be reported immediately to KSITM.
- Access to data or information under this policy shall not violate any Act or Rules of Government of India and Government of Kerala.
- KSDP would be governed by the following legal instruments:
    - National Data Sharing and Accessibility Policy (NDSAP)-2012
    - THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
    - Information Technology Act, 2000 and its amendments.
    - Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
- **Sector-Specific Regulations:** "Where applicable, departments must also comply with sector-specific data management and privacy regulations mandated by relevant Central or State Acts and Rules."

19. DISPUTE RESOLUTION

The Electronics & Information Technology Department (E& ITD) would be the Nodal Department for all matters connected with overall co-ordination, formulation, and implementation and monitoring of the policy.

In the event of any conflict related to data sharing or access, the State Level Committee shall serve as the initial arbitrator. The Apex Committee shall act as the final appellate authority for resolving grievances raised by both departmental entities and external (non-government) stakeholders.

20. Conclusion

The Kerala State Data Policy (KSDP) is designed to benefit a diverse range of stakeholders, including the various Government Departments, policymakers, research organizations and academia by fostering better governance, driving innovation, and creating new employment opportunities. This policy aims to secure Kerala’s prosperity and sustainable growth in the years to come.

Through KSDP, the Government of Kerala envisions creating a unified platform that provides users with seamless access to data and information tailored to their needs. The Electronics & Information Technology Department will amend the policy's/ guidelines’ scope and objectives as per recommendations from the Apex Committee, or to align with technological advancements and the evolving requirements of the State Government.