

# **DATA POLICY**

**CENTRE FOR COASTAL MANAGEMENT**

**UNIVERSITY OF CAPE COAST, GHANA.**

## **CONTENT**

<b>TITLE</b>	<b>PAGE</b>
The Rational	2
Data Management Structure	3
Data Categories and Governance	4
Privacy Policy	9
Intellectual Property	11
Copyright Policy	11

## **1. The Rational**

The goal of this Policy is to support academic freedom, excellence and innovation to translate knowledge and research into sustainable technologies for development.

The Policy is meant to guide data management, data monitoring and data use practices at the Centre for Coastal Management of the University of Cape Coast, Ghana. The Centre is hereafter referred to as CCM.

The Policy applies to:

- a) all data and information, processed or in raw form, stored on all CCM infrastructure, including on-campus equipment, offsite locations and equipment, and in the cloud.
- b) all data and information, processed or in raw form, collected with the support of CCM.

The Policy is guided by:

- a) African Union Data Policy Framework, 2022, endorsed by the African Union Executive Council Decision with reference EX.CL/Dec.1144(XL)
- b) UNESCO's Intergovernmental Oceanographic Commission guidelines for research data management (IOC/2016/MG/73).

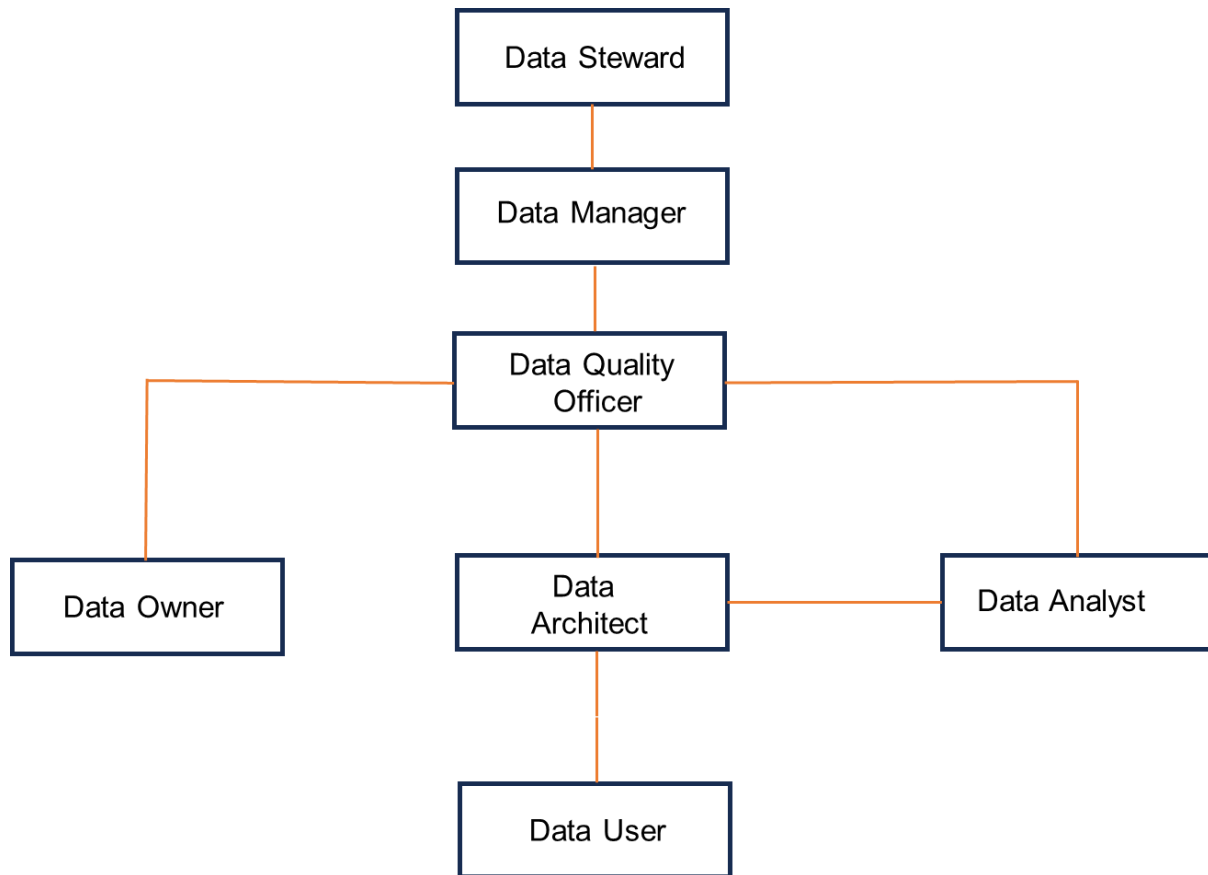
The Policy is subject to the relevant provisions:

- a) Ghana law, including Patent Act, 2003 (Act 657); Copyright Act, 2005 (Act 690); Data Protection Act, 2012 (ACT 843); Trademarks Act, 2004 (Act 664); Industrial Designs Act, 2003 (Act 660); and Protection Against Unfair Competition Act, 2000 (Act 589)
- b) Intellectual Property Policy of University of Cape Coast
- c) Research Policy of University of Cape Coast
- d) Information and Communications Technology Policy of University of Cape Coast.

This Policy document may be augmented from time to time by statements of policy or practice arising out of new, evolving media or technology.

## 2. Data Management Structure

Figure 1 describes the data management task allocation, coordination, and supervision employed by CCM.



**Figure 1.** CCM Data Management Structure

The functional roles of members on CCM data management structure are defined as follows:

- a) Data steward – this refers to data governance framework, decision-making authority, and accountability mechanisms within CCM.
- b) Data manager – a designated data auditor who assesses the quality and usefulness of dataset submitted to CCM.
- c) Data quality officer – responsible for data quality assurance and data quality control. This officer shall take appropriate measures to address suspected copyright infringement, in following with relevant laws of Ghana.
- d) Data owner –refers to individuals or entities that submit data to CCM for archiving; these individuals and entities are also known as data producers by this Policy.

- e) Data architect – shall periodically review the data infrastructure of CCM and implement solutions to improve data management strategies of the Centre.
- f) Data analyst – shall gather, clean, organize, and analyse datasets using relevant techniques – statistics, machine learning, etc. – to glean useful information to support decision-making processes of CCM.
- g) Data user – individuals and entities that access and use data from CCM

### **3. Data Policy Categories and Governance**

#### **3.1 *Data quality control and quality assurance***

This shall seek to uncover and address anomalies such as wrong methodologies and missing information that may compromise the reliability of datasets. They refer to actions of the following:

- a) Data producers:
  - i. shall collect research data using verifiable, acceptable scientific method
  - ii. shall provide complete, accurate, up-to-date and not misleading research data
  - iii. shall collect data in a responsible, ethical manner
  - iv. are required to provide current version of datasets previously archived with CCM to ensure data quality standard at the Centre
  - v. shall provide complete, accurate, up-to-date and not misleading personal data
  - vi. shall submit data guarantor. For datasets that are not yet published by indexed, peer-reviewed outlets, the data guarantor shall be an official person – research supervisor, head of research laboratory, academic department, etc. – who can provide formal, written assurance confirming reliability and accuracy of the data. For datasets that are previously published in full or in an analysed form by indexed, peer-reviewed outlets, the data guarantor shall be the digital object identifier (doi) of the publication.
- b) Data manager shall:
  - i. check for the accuracy and quality of datasets submitted to CCM. The criteria for this data validation shall include checking for the wholeness of datasets and their associated metadata

- ii. return datasets that do not pass validation tests prescribed by Section 3.1.b.i above to data authors/providers correction and resubmission

c) Data users shall:

- i. access data legally
- ii. use the data transparently, fairly and lawfully
- iii. acknowledge data source
- iv. respect intellectual property
- v. comply with relevant privacy laws and regulations governing the collection, processing, storage, and sharing of personal and sensitive data. This includes obtaining necessary consents, implementing appropriate security measures, and honouring the individual rights of data providers and authors
- vi. establish policies and procedures for data retention and disposal, ensuring that data is retained only for the necessary duration and securely disposed of when no longer needed
- vii. are liable to ensure the accuracy, completeness, and integrity of the data accessed. This includes validating data, and conducting necessary data cleansing activities.
- viii. use data for commercial purpose(s) only with the full, complete consent of data provider(s) and/or CCM.

### ***3.2 Data Accessibility***

Persons accessing data and information, processed or in raw form, from CCM:

- a) shall agree to share personal data before accessing data
- b) shall agree to terms of use of the data
- c) are obliged to obtain the data lawfully using prescribed means or protocols
- d) shall agree to process the data lawfully.

### ***3.3 Data Processing***

This refers to lawful processing and usage of data and information, processed or in raw form, obtained from CCM.

- a) Data users shall treat accessed data as confidential

- b) Personal information of data authors/providers shall not be disclosed unless required by law, or in the course of a legal duty
- c) Data users shall acknowledge data source by giving appropriate citation and acknowledgement
- d) Data may be repurposed in a responsible, ethical and lawful manner.

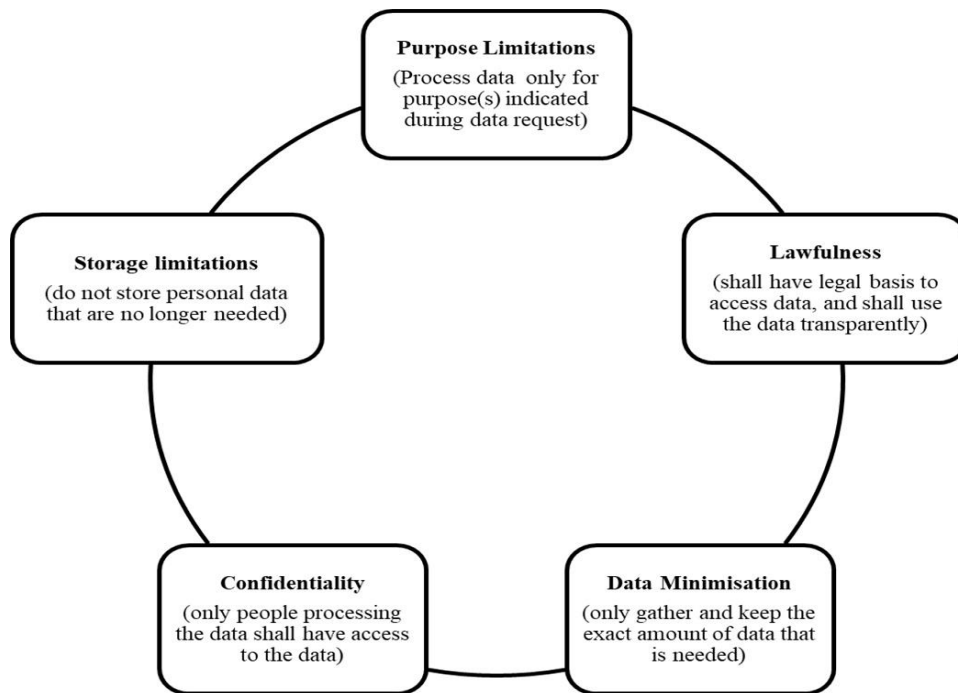
### ***3.4 Data Sharing and Disclosure***

- a) Accessed data may not be disclosed unless required by law or in the course of a legal duty
- b) Users shall share data with third parties only with the prior knowledge or authorisation of data authors/providers
- c) No commercial use of data is allowed without prior knowledge or authorisation of data authors/providers
- d) Appropriate measures shall be taken to clarify circumstances under which personal information is shared with third parties such as service providers, business partners, research collaborators or regulatory authorities.

### ***3.5 Data Protection and Security***

These policies are designed to ensure confidentiality, integrity, and availability of datasets archived with CCM. They cover the following measures:

- a) Information security
  - i. CCM implements physical data protection safeguards to ensure the protection of devices and locations which collect, process, store, and share data files and records
  - ii. Persons with authorised access data files are bound by the principles of data protection in Figure 2.



**Figure 2:** Data protection principles of CCM

- iii. Persons with authorised access shall not infringe upon the privacy rights of data subjects and data providers
- iv. Personal data shall be processed in a lawful and ethical manner
- v. Personal data shall be processed in compliance with data protection legislation of Ghana
- vi. Unless otherwise provided by law, data providers may object to the processing of their data

b) Data classification

Data are categorised for protection and identification based on the following criteria:

- i. Sensitivity – refers to data that might results in loss of an advantage or level of security if unduly disclosed
- ii. Criticality – data deemed essential for success and must be guarded
- iii. regulatory requirements – data required by regulatory agencies of CCM.

c) Data handling and transfer

- i. Data shall be transferred in a secured manner using approved authorisation both on-premises and in the cloud

- ii. Data shall be encrypted where applicable
  - iii. Data shall be handled following principles in Article 3.4.a of this Policy
  - iv. Data generated with external funding support shall be managed in accordance with prevailing agreement(s)
- d) Password and authentication
- CCM adheres to the following password policies:
- i. Users are required to use passwords containing 8 – 64 characters.
  - ii. Usage of ASCII/Unicode characters (including space and emojis) is encouraged
  - iii. Stored passwords are hashed and salted, and never truncated
  - iv. Periodic password updates
  - v. Multi-factor authentication
- e) Incidence response
- CCM adheres to strict incident reporting and response procedures. This includes incident escalation processes, data breach notification protocols, and steps for mitigating and recovering from security incidents.
- f) Employee awareness and training
- i. training on data security is conducted periodically for all CCM employees and associates. The training shall emphasise best security practices, potential risks, and roles and responsibilities of stakeholders in maintaining data security
  - ii. Security warning is displayed on all sensitive and critical data storage points
- g) Vendor and third-party security
- i. All contractors, vendors and suppliers are required to comply with the data security requirements and expectations of this policy
  - ii. All data tools are accessed for compliance with this policy before subscription
  - iii. Data tools acquired through contractual-based services are owned and hosted by CCM
- h) Data backup and recovery
- i. CCM undertakes backup, test backups and institute recovery procedures to ensure data availability in case of accidental loss, system failures, or other disruptions.



- ii. Data backup and recovery shall be implemented by data management team. The data management team at CCM shall comprise Data Manager, Data Quality Officer and other qualified person(s) appointed by Data Steward
  - iii. Data managed on third party platforms shall be periodically backed up
- i) Monitoring and auditing
- i. Appropriate monitoring and auditing practices are implemented to detect security vulnerabilities, unauthorized access, unauthorized activity and/or policy violations.
  - ii. This shall involve implementing security information and event management (SIEM) systems and periodic security assessments
  - iii. Data Quality Officer conducts privacy impact assessments, and implements internal auditing processes to safeguard the interest of data providers and all stakeholders.

#### **4. Privacy Policy**

This section addresses the collection and use of data for teaching and extension services, research, communication, analytics, marketing, and other obligations of CCM. It addresses the following:

**a) *Personal Data***

This includes names, contact details, demographic information, and browsing behaviour.

- i. Data providers shall be informed about the basis for data collection and use
- ii. Personal data shall be collected, used, handled, and protected in a lawful, transparent and ethical manner, in line with relevant laws of Ghana
- iii. Data providers shall have the right to know how personal information is used and shared
- iv. Data providers shall have the right to request the deletion of personal information. This right shall not be granted when CCM is prohibited by law or legal duty.
- v. Data providers shall have the right to opt-out of the sharing of their personal information. This right shall not be granted when CCM is prohibited by law or legal duty.

- vi. Data providers shall have the right to correct inaccurate personal information provided to CCM
- vii. Data providers shall have the right to limit the use and disclosure of their sensitive personal information. This right shall not be granted when CCM is prohibited by law or legal duty
- viii. CCM shall promote data minimization principles, ensuring that only necessary and relevant personal data is collected, used and retained.

**b) *Research Data***

This refers all research data, processed or in raw form, submitted to CCM.

- a) Persons outside of CCM who are not supported by CCM shall voluntarily choose to submit research data without any pressure or coercion
- b) Persons who obtain research data through CCM and/or with the support of CCM are obliged to submit the data outcome of the research to CCM for management
- c) Data providers shall adhere to data protection principles provided in Figure 2 under Section 3.4.
- d) Data providers have the right and moral responsibility to correct inaccurate research data previously submitted to CCM
- e) Data providers shall be informed about the basis for data collection and use
- f) Data providers have the right to know how their research data is used and shared
- g) Data providers shall have the right to request the deletion of research data archived with CCM. Such requests shall be done with reasonable justification. The request shall not be granted when CCM is prohibited by law or legal duty.
- h) Data generated between CCM and other organizations are bound to be retained in line with principles in this policy unless after the expiration of any agreement
- i) Data retention shall comply with all relevant provisions in Ghana's Data Retention Act, 2012 (ACT 843).

**c) *Cookies and Tracking Technologies***

Cookies or tracking technologies may be deployed when necessary, particularly for system improvement and performance.

**5. Intellectual Property**

- a) Management of intellectual property arising from the use of data submitted to CCM shall conform with the UCC IP Policy
- b) Providers of research data shall hold intellectual right to the data

**6. Copyright Policy**

- a) CCM shall hold copyright to all datasets submitted by data providers
- b) Data providers shall hold moral right to their data. This includes the right to be identified as authors, to prevent any derogatory treatment of their work, and to privacy, for example by preventing publication of personal data
- c) Data providers shall hold economic rights to their data. This includes the right to copy the data, the right to issue copies of the data to the public, the right to rent or lend the data to others, and the right to make an adaptation of the data.

Articles 6 d – 6 g below apply to all data collected by or with funding and/or in kind support from CCM through internal, external, or international sponsoring agencies.

- d) All data collected through CCM or with support from CCM are considered to be owned by CCM, and by extension the University of Cape Coast as stipulated in UCC Intellectual Property Policy (Section 6)
- e) Data collected within national exclusive economic zones (EEs) through CCM or with support from CCM are owned by CCM; Representative of respective countries may be given access upon request
- f) Data collected in areas beyond national jurisdiction through CCM or with support from CCM will be owned by CCM. Individuals and organisation may be given access upon request

- g) All workers including research scientists, consultants and students of CCM shall be obliged to submit raw, statistically undescribed outcomes of all research activities to CCM in pursuant of Sections 4 f iv – vii of this Policy
- h) Use of digitally accessed data including online publications, websites, social media, and digital assets shall be used guidelines on proper attribution, respecting digital rights management, and avoiding unauthorized use or distribution of digital content.
- i) Copyright Awareness – CCM shall educate employees about the basics of copyright, and equitable use of data
- j) Licensing and Permissions – There shall be a process for obtaining licenses and permissions to use copyrighted materials when necessary. It shall include procedures for identifying and acquiring the appropriate rights and ensuring compliance with licensing terms and conditions, in line with UCC Policy on intellectual property, where applicable.
- k) Copyright Infringement Reporting – Data Quality Officer shall report and address suspected copyright infringement, in following with relevant laws of Ghana. There shall be consequences for copyright infringement.