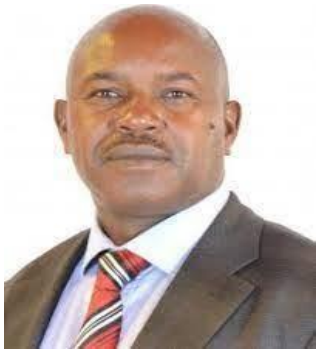
DATA PROTECTION POLICY

Wildlife Research and Training Institute
P.O. Box 842-20117, Naivasha, Kenya
Telephone: (+254) 050 2020577
Mobile: (+254) 0700 000321 /0731 919 465
Website: www.wrti.go.ke
Email: director@wrti.go.ke, wrti@wrti.go.ke

Table of Contents

FOREWORD



The Wildlife Research and Training Institute is mandated by Government to undertake research in the Wildlife sector to guide policy making. The Institute processes both wildlife and personal data and is committed to upholding the highest standards of data protection. This data protection policy speaks to that commitment and sets a framework in line with the laws of the land on how we shall process and control data in the Institute.

The purpose of this policy is to provide guidelines on how the Institute shall process the personal data of its staff, trainees, research participants, suppliers and other third parties in compliance with data protection law and to protect the data subject's rights. The policy shall apply to all personal data the Institute processes regardless of the format or media on which the data is stored or to whom it relates. This Data Protection (DPP) Policy has been developed in line with Kenya Constitution of Kenya, the Data Protection Act, Access to Information Act and the Data Protection General Regulations. It is anticipated that the full implementation of this Data protection policy will safeguard the processing and controlling of data regarding wildlife research and training.

The Institute recognizes that protecting individuals through legitimate and responsible processing and using their personal data is an imperative human right. The Institute is committed to complying with the legal requirements contained in the Data Protection Act and other required legislation.

..... **DATE:** 16th May, 2025

DR DAVID NKEDIANYE
CHAIR, BOARD OF THE INSTITUTE

PREFACE

This data protection policy is a document with regulations and procedures that shall be adopted to protect and secure all data consumed, managed, and stored by the Institute. The policy covers all personal data that the Institute holds for either past, current or prospective persons in either electronic or paper format, from when it is created to when it is either destroyed or permanently preserved. It provides the rules of personal data protection, including related obligations of staff, trainees, research participants, suppliers and other third parties in ensuring responsible processing of personal data. This policy demonstrates the Institute's commitment to ensuring adequate level of protection and privacy of personal data as prescribed in the Data Protection Act.

This policy document is intended to ensure that the Institute;

- Processes personal data with care;
- Complies with existing data protection laws and with good practice;
- Protects its reputation by ensuring the personal data entrusted to it is processed in accordance with data subjects' rights;
- Protects itself from risks of personal data breaches and other breaches of data protection law.

This policy shall apply to all members of the Institute, including staff, trainees, parents, guardians, sponsors, associates, contractors, partners, interns, regulatory bodies and other parties that interact with the Institute.

.....
DR PATRICK OMONDI, OGW
DIRECTOR/CEO

DATE: 16th May, 2025

LIST OF ACRONYMS AND / OR ABBREVIATIONS

DPA:	Data Protection Act
DPC:	Data Protection Committee
DPIA:	Data Protection Impact Assessment
DPL:	Data Protection Law
DPO:	Data Protection Officer
DPP:	Data Protection Policy
ODPC	Office of The Data Protection Commissioner
PD:	Personal Data
WRTI	Wildlife Research and Training Institute

DEFINITION OF TERMS

A minor: means a person who has not attained the age of majority as per Kenyan law.

Consent: means agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by clear positive action, signifies agreement to the processing of personal data relating to them.

Data controller means a natural or legal person, public authority, agency, or other body which has the authority to oversee the management of and to determine the purposes for the processing of personal data.

Data processor means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.

Data processing means converting data into information. This includes collecting, recording, rationalizing, storage, alteration, retrieving, using, transmission, dissemination, erasure, or destruction of data.

Data Subject: means a living, identified or identifiable natural person who is the subject of personal data.

Data Protection Impact Assessment (DPIA): means tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving processing personal data.

Data Protection Officer (DPO): means a DPO is responsible for advising the Institute (including its employees) on their obligations under Data Protection Act, for monitoring compliance with the data protection policy.

DPP: means Data Protection Policy.

Data transfer: means all acts that make personal data accessible to third parties outside of the Institute on paper, via electronic means, on the internet, or through other means.

Data Transfer Agreement: means an agreement between the Institute and a third party that states the terms and conditions of use of personal data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues.

Health data: Data related to the state of physical or mental health of the data subject

Institute: means Wildlife Research and Training Institute.

Profiling: means any form of processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Research: means any creative work undertaken on a systematic basis to increase the stock of knowledge, including knowledge of man, knowledge on man, culture and society, and the use of this stock of knowledge to devise new applications.

Sensitive personal data: means data revealing the natural person's race, health status, ethnic, social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

Staff/Employee: means any person who at the time of creation of the this policy is under contract of employment with the institute including but not limited to whether on Contract, permanent and pensionable, on secondment, affiliates, students undertaking work for the Institute, interns.

Student/Trainee: means any individual registered for an approved course in the Institute including attachees and those under exchange program in the Institute.

Third party: natural or legal person, public authority, agency or other body, other than the data subject, the Institute or persons who, under the direct authority of the Institute are authorised to process personal data.

Personal Data: means any information identifying a data subject or information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers the Institute possess or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: means any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.

Privacy by Design and Default: means implementing appropriate technical and organisational measures effectively to ensure compliance with the Data Protection Policy.

Privacy Notices: means separate notices setting out information that may be provided to data subjects when the Institute collects information about them. These notices may be general privacy statements applicable to a specific group of individuals (for example,

employee, trainee and donor privacy notices or the website privacy policy), or they may be stand-alone, one-time privacy statements covering processes related to a specific purpose.

Processing or Process: means any activity that involves the use of personal data. It includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.

Pseudonymisation or Pseudonymised: means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Personal data: means Name, Phone number Birth certificate and location

Sensitive Data : include health status, biometric data, ethnicity and marital status

1.0: Introduction

1.1 The Institute is a Government Research and training Corporation mandated to coordinate and undertake wildlife research and training in the country in accordance with section 51 of the Wildlife Conservation and Management Act.

1.2 The Institute was established to provide reliable scientific information on emerging wildlife conservation and management challenges and enhance capacity in the wildlife sector through training.

1.3 The Institute uses the data in its possession to plan and execute its mandate and make decisions in executing the daily operations.

1.4 In accordance to the Constitution of Kenya and the Data Protection Act the Institute is obligated to control and process personal data

1.5 This policy will guide the Institute process and control personal data in accordance to the existing laws.

2.0 Purpose of the Data Protection Policy

2.1 This policy aims at providing the Institute with proper guidelines in data management as well as ensuring that the Institute complies with the legal requirements as per the Data Protection Act (Cap.411C).

3.0 Scope of Data Protection Policy

3.1 This policy shall apply to data collected, received, and stored on the Institute-owned physical and electronic databases and resource center. It shall apply to all staff, students, parents, guardians, sponsors, associates, contractors, partners, interns, regulatory bodies and other parties that interact with the Institute.

3.2 It shall also apply to all users of the Institute's applications, software, databases, websites, social media platforms, and all other such like resources.

3.3 This policy shall cover all data/ information collection tools of the Institute including but not being limited to performance assessment tools, employee databases, wildlife databases, student databases, research databases, mobile applications, research publications, and communication tools such as photos, videos, social and mainstream media.

4.0 Governance Framework

The governance framework for this policy shall be;

i. Board of the Institute
ii. Director/CEO
iii. Data Protection Committee
iv. Data Protection Officer
v. Data Custodians
vi. Staff

5.0 Legal Framework

i. Constitution of Kenya.
ii. Data Protection Act (Cap.411C).
iii. The Computer Misuse and Cybercrimes Act (Cap.79 C).
iv. Kenya Information and Communications Act (Cap.411A).
v. The National ICT Policy,
vi. The Copyright Act (Cap. 130).
vii. Other relevant legal provision and Government policies that may come into force after initial implementation of this ICT Policy.

6.0 Roles and Responsibilities for Implementation

6.1 Board of the Institute

The board shall—

(a) give policy direction on data management and protection in the Institute; and
(b) give guidance on the policy direction, provide budgetary allocation for its implementation and conduct its oversight implementation.

6.2 The Director/Chief Executive Officer

The Director/Chief Executive Officer shall—

(a) Appoint the Data Protection Officer in accordance to the Act;
(b) Appoint Data Protection committee to guide on the implementation of this policy;
(c) Provide resources for the implementation of this policy;
(d) Register and Renew the Institute as a controller and processor of data with the office of the Data Commissioner;
(e) Ensure the security of data as provided in the guidelines;
(f) Notify the Office of the Data Commissioner within seventy two hours in case of a data breach; and
(g) Ensure that data is not transferred outside the Country as per the Public Data Regulations.

6.3 Data Protection Committee

The Data Protection Committee shall—

(a) Steer the implementation and monitoring of the Institute's Data Protection policy to foster personal data privacy;
(b) Review and make recommendations to the Institute on the policies, procedures and code of practice in relation to personal data handling and monitoring the implementation of these policies, procedures and code of practice;
(c) Develop a personal data inventory for implementation by all units of the Institute with access to personal data and monitoring the periodic personal data inventory review exercise;
(d) Initiate and monitor the periodic risk assessment of all operating units of the Institute and the privacy impact assessment, when deemed appropriate;
(e) Promote staff and students' awareness of data protection and provide training and education to staff members with duties for handling personal data;
(f) Formalise and monitor the mechanism for reporting and handling a data breach incident;
(g) Review the effectiveness of the Institute's data protection policy where necessary; and
(h) Report to the Director/CEO from time to time on matters relating to the Institute's compliance in relation to data protection.

6.4 Data Protection Officer

A Data Protection Officer (DPO) who shall—

(a) Oversee the implementation of the Data Protection Act and related regulations;
(b) Conduct trainings to staff and trainees in regarding to data protection practices;
(c) Give guidance on the conduct of a data protection impact assessment;
(d) Advise the Institute and its staff of its obligations under DPP;
(e) Monitor compliance with this policy and other relevant data protection laws;
(f) Provide advice where requested on data protection impact assessments;
(g) Cooperate with and act as the contact point for the Institute; and
(h) Receive complaints that relate to personal data and communicate to the relevant authorities with consultation from the Director.

The DPO shall, in the performance of his or her tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of the processing.

6.5 Data User

Data User shall be staff from the training, research and corporate services division handling data in the Institute. Data users shall be responsible for controlling and processing data in compliance with this policy and to the best interest of the Institution.

6.6 Data Custodians

Data Custodians shall be staff working in the technical departments from Information Communication Technology and Records Management who shall—

(a) Ensure proper access controls are put in place in accordance to the Data Protection Act;
(b) Carry out regular backups of the Institute's Data;
(c) Validate the data validity;
(d) Backup and maintain the database and servers holding the Institution's data;
(e) Ensure compliance with security policies safeguarding data within the Institute;
(f) Provide secure storage and encryption to data while in storage or on movement;
(g) Access data using the existing guidelines; and
(h) Undertake data classification compliance in conjunction with the data owners

6.7 The Staff

The staff of the Institute shall be responsible for adherence to the data protection policy by accurately capturing, processing and controlling data within the Institute. Employees shall report through the authorized channels any attempted data breaches in the Institute.

7.0 Objectives of Data Protection Policy

7.1 The Data Protection Policy shall ensure personal data and overall data protection within the Institute and to ensure the privacy of personal data is upheld.

7.2 The Policy shall guide how personal data must be processed and the Institute's expectations for all those who process personal data on its behalf. Further, this will ensure that the Institute complies with existing data protection laws and with good practice.

7.3 The Policy protects the Institute's reputation by ensuring personal data entrusted to it is processed in accordance with data subjects' rights.

7.4 The Policy protects the Institute from risks of personal data breaches and other breaches of data protection law.

8.0 Policy Statement

8.1 The Institute shall comply with the legal requirements that relate to the control and processing of data held within the Institute.

8.2 This policy shall provide the guidelines which the Institute shall apply in handling personal data to ensure compliance with the existing laws.

9.0 Rationale

9.1 This policy shall guide the Institute in ensuring that the data collected, processed, controlled is of high quality and is secured properly.

9.2 The policy will also ensure that the data protection practices are put in place in compliance with the relevant laws, regulations and standards.

10.0 Data Protection Guidelines

10.1 The Institute has established this policy in line with the Institute strategic plan and relevant laws. The policy shall be implemented through the laid down procedures and guidelines in line with existing data sharing protocols and existing applicable laws related to wildlife data.

10.2 The Institute shall in dealing with personal information and data ensure that the information/ data is processed:

(a) without infringing the privacy rights of the data subject;

(b) in a lawful manner; and

(c) in a reasonable manner.

11.0 Implementation

11.1 All staff and relevant third-parties shall comply with the requirements of this policy.

12.0 Policy Review

12.1 This policy shall be reviewed every three years or as need arise.

ANNEX 1: DATA PROTECTION GUIDELINES

1.0 DATA MANAGEMENT

The Institute shall collect, securely store or use personal data for a lawful, specific and explicitly defined purpose.

(a) The Institute shall collect personal data directly from the data subject.

(b) The Institute shall collect personal data indirectly where—

(i) the data is contained in a public record;

(ii) the data subject has deliberately made the data public;

(iii) the data subject has consented to the collection from another source;

(iv) the data subject has an incapacity and the guardian appointed has consented to the collection from another source; or

(v) the collection from another source would not prejudice the interests of the data subject.

(c) The Institute shall collect data from another source if data is necessary for—

(i) the prevention, detection, investigation, prosecution and punishment of crime;

(ii) the enforcement of a law which imposes a pecuniary penalty; or

(iii) the protection of the interests of the data subject or another person.

1.1 Data Catalogue

The Institute shall:

(i) Generate a data catalogue to include all data it owns which will provide the technical classifications of data;

(ii) The catalogue will provide information regarding the ownership, quality, description, purpose and other required data dimensions;

(iii) The catalogue shall create a glossary of terms within the data catalogue; and

(iv) Regularly update the catalogue with new datasets within the Institute.

1.2 Principles of Data Protection

The Institute shall ensure that personal data is:

(a) Processed in accordance with the right to privacy of the data subject;

(b) Processed lawfully, fairly and in a transparent manner in relation to any data subject;

(c) Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(d) Adequate, relevant, limited to what is necessary for relation to the purposes for which it is processed;
(e) Collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
(f) Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
(g) Kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
(h) Not transferred outside the Institute unless there is proof of adequate data protection safeguards or consent from the data subject.

1.3 Data Storage

The Institute shall:

(i) provide resources to ensure that data and information systems are held in a safe and secure;
(ii) develop and execute a data migration plan to safeguard the Institute's data;
(iii) establish a continuous monitoring plan for data and information storage systems;
(iv) ensure data is securely backed up according to the backup policy as per the ICT Policy;
(v) develop and implement a disaster recovery plan aimed at minimized service disruption; and
(vi) dispose of media containing data that need to be erased with the approval from the Head of ICT.

1.4 Duty to Notify

The Institute shall, before collecting personal data, in so far as practicable, inform the data subject of—

(a) rights of the data subject;
(b) personal data is being collected; images, videos
(c) purpose of personal data being collected;
(d) transfer of personal data to third parties including details of safeguards adopted;
(e) third-party contacts and whether any other entity may receive the collected personal data;
(f) technical and organisational security measures taken to ensure the integrity and confidentiality of the data;
(g) data being collected pursuant to any law and whether such collection is voluntary or mandatory; and
(h) consequences, if any, where the data subject fails to provide all or any part of the requested data.

2.0 PROCESSING OF PERSONAL DATA

The Institute shall not process personal data unless:

(a) The data subject consents to the processing of one or more specified purposes; or

(b) The processing is necessary for:

(i) performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
(ii) compliance with legal obligation to which the Institute is subject;
(iii) protection of the data subject interests or another data subject;
(iv) the performance of a task carried out in the public interest or in the exercise of official authority vested in the Institute;
(v) performance of any task carried out by a public authority;
(vi) the exercise, by any person in the public interest, of any other functions of a public nature;
(vii) legitimate interests pursued by the Institute by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
(viii) the purpose of historical, statistical, journalistic, literature and art or scientific research.

(c) Processing of personal data shall be in accordance with the purpose of collection.

(d) A third party who contravenes the provisions of this policy commits an offence.

2.1 Rights of a Data Subject

The Data Subject has the right to:

(a) be informed
(b) access
(c) withdraw consent;
(d) rectification;
(e) erasure; and
(f) restrict processing.

2.2 Exercise of Rights of Data Subjects

A right conferred on a data subject shall be exercised—

(a) where the data subject is a minor, by a person who has parental authority or by a guardian;

(b) where the data subject has a mental or other disability, by a person duly authorised to act as their guardian or administrator; or

(c) In any other case, by a person duly authorised by the data subject.

2.3 Processing of Data Relating to a Minor

(a) The Institute shall not process personal data relating to a minor unless:

(i) the minor's parent or guardian gives consent; and

(ii) the processing is in such a manner that protects and advances the rights and best interests of the minor.

(b) The Institute shall incorporate appropriate mechanisms for age verification and consent to process a minor's personal data.

(c) Mechanisms contemplated under sub-section (b) shall be determined based on:

(i) available technology;

(ii) volume of personal data processed;

(iii) proportion of such personal data is likely to be that of a minor;

(iv) possibility of harm to a minor arising out of the processing of personal data; and

(v) such other factors as may be specified by the Institute.

(d) In the event that the Institute provides services to a minor, the Institute shall be required to obtain parental consent as set out under sub-section (a) (i).

2.4 Restrictions on Data Processing

The Institute shall at the request of a data subject, restrict the processing of personal data where:

(i) the accuracy of the personal data is contested by the data subject for a period enabling the Institute to verify the accuracy of the data;

(ii) personal data is no longer required for the purpose of the processing unless the Institute requires the personal data for the establishment, exercise or defence of a legal claim;

(iii) processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

(iv) the data subject has objected to the processing, pending verification as to whether the legitimate interests of the Institute override those of the data subject.

Where the processing of personal data is restricted under this section:

(v) the personal data shall, unless the data is being stored, only be processed with the data subject's consent or for the establishment, exercise or defence of a legal claim, the protection of the rights of another person or for reasons of public interest; and

(vi) the Institute shall inform the data subject before withdrawing the restriction on processing personal data.

The Institute shall implement mechanisms to ensure that time limits are established for the rectification, erasure or restriction of processing of personal data or for a periodic review of the need for the storage of the personal data is observed.

3.0 RESPONSIBILITIES ON DATA PROTECTION

3.1 Institute Responsibilities

The Institute shall establish and implement policies and procedures to comply with data protection laws.

3.2 Staff Responsibilities

The employee's who process personal data about students, staff, applicants, alumni or any other individual shall comply with the requirements of this policy.

Staff members shall ensure that:

(i) all personal data is kept securely;

(ii) no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;

(iii) personal data is kept in accordance with the Institute Records Policy;

(iv) any queries regarding data protection, including subject access requests and complaints, are promptly directed to Data Protection Officer;

(v) any data protection breaches are swiftly brought to the attention of the Data Protection Officer;

(vi) where there is uncertainty around a data protection matter, advice is sought from the Data Protection Officer;

(vii) where staff members are responsible for supervising students doing work which involves processing personal information (for example, in research projects), they shall ensure that those students are aware of the Data Protection principles; and

(viii) staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data shall seek advice from the Data Protection Officer.

3.3 Third-Party Data Processors

Where external companies are used to process personal data on behalf of the Institute, the responsibility for the security and appropriate use of that data shall remain with the Institute.

Where a third-party data processor is used:

(i) a data processor shall be appointed to provide sufficient security measures to protect the processing of personal data;

(ii) reasonable steps shall be taken to ensure security measures are in place; and

(iii) a written contract establishing what personal data shall be processed and for what purpose shall be set out.

The Institute shall inform the external company being engaged as a data processor of the data protection policies.

3.4 Contractors

For purposes of this section, Contractor means a person engaged by the Institute through a service level agreement or equivalent which provisions require processing of personal data.

All Contractors shall provide the Institute with the Data in accordance with the terms of this Policy. In so far as personal data is provided by a Contractor to the Institute, and/or Processed by the Institute, both the Contractor and the Institute qualify as independent Controllers for such Processing.

The terms of engagement between the Institute and Contractor shall stipulate the responsibilities of the Institute and that of the Contractor. The Contract shall stipulate that: Personal data shall be collected, processed and transferred in accordance with the DPP and any other applicable data protection laws.

3.5 Short-Term and Voluntary Staff

The Institute shall be responsible for the use of personal data by anyone working on its behalf. Short-term or volunteer staff shall be appropriately vetted for the data they shall be processing.

The Institute shall ensure that:

(i) any personal data collected or processed in the course of work undertaken for the Institute is kept securely and confidentially;

(ii) all personal data is returned to the Institute on completion of the work, including any copies that may have been made. Alternatively, the data is securely

destroyed, and the Institute receives notification in this regard from the contractor or short- term/voluntary member of staff;

(iii) the Institute receives the prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;

(iv) any personal data made available by the Institute, or collected in the course of the work, is neither stored nor processed outside the Institute unless written consent to do so has been received from the Institute; and

(v) all practical and reasonable steps are taken to ensure that contractors, short-term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

3.6 Student Responsibilities

Students shall be responsible for:

(i) familiarising themselves with this policy when they enroll with the Institute; and

(ii) ensuring that their personal data provided to the Institute is accurate and up to date.

4.0 OBJECTING TO PROCESSING

A data subject shall have a right to object to processing their personal data unless the Institute demonstrates compelling legitimate interest for the processing, which overrides the data subject's interests, or for the establishment, exercise or defense of a legal claim.

4.1 Commercial use of data

A person shall not use, for commercial purposes, personal data obtained from a data subject pursuant to the provisions of this policy unless the person:

(a) has sought and obtained express consent from a data subject; or

(b) is authorised to do so under any written law, and the data subject has been informed of such use when collecting the data from the data subject.

Where the Institute uses personal data for commercial purposes, it shall, where possible, anonymize the data in such a manner as to ensure that the data subject is no longer identifiable.

4.2 Right to Data Portability

A data subject shall have the right to—

(i) receive personal data concerning them in a structured, commonly used and machine-readable format;

(ii) transmit the data obtained under sub-section (i) to a third party without any hindrance;
(iii) have the personal data transmitted directly from the Institute to the third party;

The right under this section shall not apply in circumstances where—

(a) processing may be necessary for the performance of a task carried out in the public interest or the exercise of official authority; or

(b) it may adversely affect the rights and freedoms of others.

The Institute shall comply with data portability requests within reasonable timelines; where costs are incurred, the data subject shall bear the cost.

5.0 SECURITY

The Institute shall implement a high level of data security that is appropriate to the risks presented by the nature and processing of personal data taking into account the level of technology available and existing security conditions as well as the costs of implementing additional security measures.

Personal data will be filed and stored in a way that is accessible only to authorized staff and transferred only through the use of protected means of communication to ensure confidentiality.

The Institute shall take appropriate technical and organizational data security measures to ensure the confidentiality.

The nature of risks will include but not be limited to the risk of accidental or unlawful/illegitimate destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data.

Access to personal data/content/knowledge shall be restricted to authorized personnel using it in the performance of their duties at the Institute and as determined by appropriate authorization of both the staff or volunteers' supervisor and data subjects.

Personal data/content/knowledge shall not be used by any employee or staff for purposes other than the business of the Institute.

5.1 Data Breach

The Institute shall maintain a register of all data breaches, the Institute's staff shall notify the supervisor of any personal data breach, and they shall keep a record of the breach.

If a personal data breach is likely to result in personal injury or harm to a data subject, the data controller will communicate the personal data breach to the data subject and take mitigating measures as appropriate without undue delay.

In such cases, the data controller shall also notify the Director/CEO of the personal data breach. The notification will describe:

(i) the nature of the personal data breach, including the categories and the number of data subjects and data records concerned;
(ii) the known and foreseeable adverse consequences of the personal data breach; and
(iii) the measures are taken or proposed to be taken to mitigate and address the possible adverse impacts of the personal data breach.

6.0 Data Protection Impact Assessment

The Institute shall, prior to the processing, carry out a data protection impact assessment, which shall include:

(i) A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the Institute.
(ii) An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
(iii) An assessment of the risks to the rights and freedoms of data subjects.
(iv) The measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Data Protection Act taking into account the rights, and legitimate interests of data subjects and other persons concerned.
(v) The Institute shall consult the Office of Data Commissioner prior to the processing of a data protection impact assessment prepared under this section indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject.
(vi) The Institute shall submit data impact assessment reports at least sixty days prior to the processing of data.
(vii) The Institute shall adhere to set out guidelines for carrying out an impact assessment by the Office of Data Commissioner.