# IIDC DATA PROTECTION POLICY

Contents

# DATA PROTECTION POLICY

## Introduction

This policy sets out the obligations of Impact and Innovations Development Centre (IIDC), regarding data protection and the rights of all persons whose data may be collected or processed ("data subjects").

The procedure and principles set out herein must be followed at all times by IIDC, its employees, agents, contractors, or other parties working on behalf of IIDC.

## Purpose and Context

Impact and Innovations Development Centre (IIDC) is committed to a policy of protecting individuals' right to privacy in accordance with the Data Protection and Privacy Act, 2019 (including any replacement of that Act) (the "**DPPA**") . This policy sets out that commitment.

IIDC recognizes that correct and lawful treatment of Personal Data contributes to the good reputation of the organisation by demonstrating its integrity and its respect for those it deals with.

IIDC needs to process certain information about its Beneficiaries, staff, suppliers, partners and other individuals it has dealings with. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

As such, IIDC is committed not only to the letter of the law, but also to the spirit of the law, and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

## Scope

This policy encompasses all Processing of Personal Data by staff, suppliers and partners, each of whom are subject to this policy. As a matter of good practice, other organisations or agents who have access to and process Personal Data on behalf of IIDC will be expected to have read and comply with this policy.

It is the responsibility of the relevant Departments or employees who deal with such external third parties to ensure that such third parties agree in writing to abide by this policy, with support from published procedures and guidance, and from IIDC Data Protection Team.

## Development process

This policy also applies to staff, suppliers and partners who process Personal Data "off-site". Off-site Processing presents a potentially greater risk of loss, theft or damage to Personal Data. Staff, suppliers and partners should take particular care when Processing Personal Data at home or in other locations outside IIDC offices and should comply with IIDC's Regulations governing use of Computing Facilities and with the IT Security Policy and Procedures.

## 1. Policy Statement

1.1 This policy does not form part of the formal contract of employment for staff, but it is a condition of employment that employees will familiarize themselves with and act in accordance with this policy. IIDC may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be managed in accordance with IIDC's policy framework.

1.2 Any failure to follow this policy by Staff and suppliers may result in disciplinary action. Any failure by partners to follow this policy may result in their access to IIDC IT and information systems and premises being restricted or removed.

## 2. Background

2.1 The purpose of the Data Protection and Privacy Laws is to protect the rights and privacy of living individuals and to ensure that Personal Data is Processed fairly and transparently.

2.2 IIDC collects, holds and uses Personal Data relating to individuals who have/have had a relationship with the organization.

2.3 The purpose of this policy is to ensure that IIDC:

a) Operates procedures and practices that conform to the requirements of the Data Protection and privacy Laws when working with Personal Data;

b) Clearly defines responsibilities and accountability for data protection; and

c) Provides staff, suppliers and partners with the resources, knowledge, competencies and procedures to work with Personal Data in compliance with the Data Protection and privacy Laws and with this policy.

2.4 Breach of the Data Protection and Privacy Laws can lead to enforcement action by the Personal Data Protection Office, which can now impose monetary penalties on IIDC not exceeding two percent of IIDC's annual gross turnover. IIDC might also be sued by any individuals affected by the breach. In addition, individuals may also be subject to fines and criminal liability where they are found to have breached the Data Protection and Privacy Laws.

## 3. Key Data Protection Definitions.

3.1 This policy tries as far as possible to avoid using technical terms. However, there are some terms used in the Data Protection and Privacy Law that it are helpful to understand, in the context of data protection compliance. To assist such understanding, we have set out a list of key terms and their meanings below. Where these terms are used in this policy, they should be read and applied in this context;

| | |
|---|---|
| **“Data”** | Any information that is collected and/or stored by IIDC. This consists of information from events, from our partners or from field activities. |
| **"Data Subject"** | Means an individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored. |
| **“Data Processing”** | Means any operation performed upon collected data by any means including automated means including;<br>a) Organisation, adaptation or alteration of the information or data;<br>b) Retrieval, consultation or use of the information or data;<br>c) Disclosure of information or data by transmission, dissemination or otherwise making data available;<br>d) Alignment, combination, blocking, erasure or destruction of the information or data. |
| **"Data Controller"** | Means a person who alone, jointly or with other persons determines the purposes for and the manner in which personal data is processed or is to be processed.<br><br>In the context of the majority of Personal Data held by IIDC, IIDC will be the Data Controller. IIDC is therefore in position to make decisions with regard to particular Personal Data, including decisions regarding the purposes for which Personal Data is Processed and the way in which the Personal Data is Processed. |
| **“Data Collector”** | Means a person who collects personal data. In this context, IIDC is the Data collector. |

| | |
|---|---|
| **"Special/Sensitive Personal data"** | Means Personal Data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data, biometric data for the purpose of uniquely identify a person (e.g. fingerprints), data concerning physical or mental health or condition (e.g. substance abuse testing), sexual life, criminal offences, or related proceedings.<br><br>Any use of Sensitive Personal Data or Special Category Data must be strictly controlled in accordance with this policy. |
| **"Third Party"** | In relation to personal data, means a person other than the data subject, the data collector, data controller, or any data processor or other person authorized to process data for the controller or processor. |
| **"Personal Data"** | Means any data that is related to an identified or identifiable natural person from that information or from that data combined with other information in possession of IIDC.<br><br>To be identifiable means that one can be identified directly or indirectly, especially through the use of a reference like name, location, identification number or anything physical, mental, psychological, among others that express the identity of the natural person.<br><br>Such data also includes telephone number, staff ID number, details of organisations worked for and photographs (which may also constitute sensitive personal data). The data may also include expression of opinion about the individual, and of the intentions of the organization in respect of that individual. |

## 4. Legal Framework

4.1 IIDC is required by law to comply with certain rules, procedures and processes regarding the collection and processing of personal data. These laws include the Data Protection and Privacy Act 2019 and the Data Protection and Privacy Regulations 2021.

4.2 In summary, the above laws, regulations and best practices require that personal data is;

a) Processed lawfully, fairly and in a transparent manner in relation to individuals.
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes.
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
e) Kept in a form which permits identification of data subjects for no longer than is necessary for.
f) the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
g) Processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
h) The controller (or the data governance officer) shall be responsible for, and be able to demonstrate, compliance with the principles.

4.3 This policy shows, in details how IIDC will comply with the above rules.

## 5. The Data Protection Principles

5.1 The policy of IIDC is to process personal data in accordance with the applicable Data Protection and Privacy Laws and rights of individuals as set out below. All staff have personal responsibility for the practical application of the organisation's data protection policy.

5.2 The Organisation will observe the principles set out in the Data Protection and Privacy Laws in respect of the Processing of Personal Data.

5.3 Therefore, at all times during the collection, storage and processing of personal data, IIDC shall ensure that the following principles are upheld:

a) That personal data is processed lawfully, fairly, and in a transparent manner in relation to the data subject. Those responsible for Processing Personal Data (See Clause 6 which details the roles and responsibilities of various personnel.) must make reasonable efforts to ensure that Data Subjects are informed of the identity of the Data Controller (i.e. IIDC), the purpose(s) and legal basis of the Processing, any disclosures to third parties that are envisaged and an indication of the period for which the Personal Data will be kept.
b) That personal data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Personal Data will not be processed in a manner incompatible with those purposes, and Personal Data obtained for specified purposes must not be used for a different purpose. As such, further processing for archiving purposes in the public interest, or for research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

c) That personal data is collected, processed or used in a framework that is transparent and provides for the participation of the data subject.
d) That personal data is inclusive and ensures equity.
e) That personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Information that is not strictly necessary for the purpose for which it is obtained should not be collected. If Personal Data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.
f) That personal data is accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay. Personal Data that is kept for a long time must be reviewed and updated as necessary. No Personal Data should be kept unless it is reasonable to assume that it is accurate.
g) It is the responsibility of all individual staff, suppliers and partners to ensure that Personal Data held by the organization is accurate and up to date. Completion by a Data Subject of an appropriate registration or application form, etc. will be taken as an indication that the data contained therein is accurate. Individuals should notify the organization of any changes in circumstance to enable personal records to be updated accordingly. Suppliers should contact the Administrators office. Staff should contact their Human Resources representative in Human Resources. It is the responsibility of the organization to ensure that any notification regarding change of circumstances is noted and acted upon.
h) That Personal Data is not kept for longer than is necessary for the purposes for which it is used. (See Clause 25 Retention and Disposal of data).
i) That Personal Data is processed in accordance with the rights of data subjects in accordance with the Data Protection and privacy Laws (see Clause 7 on the Rights of Data Subjects).
j) That personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the DPPA to safeguard the rights and freedoms of the data subject.
k) That personal data processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. (See Clause 18 on Secure Processing of Data/Security of Data).
l) That Personal Data is not transferred to a country or a territory outside the Uganda economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the Processing of Personal Data.
m) **That personal data is innovative, constantly** innovating to ensure individuals benefit from the use of their data through better experiences, products and services, as well as the application of the most up to date best practices for the collection, use and security of personal data.

5.4 The organization should generally not Process Personal Data unless:

- It is to fulfil a contract with the individual (be this a staff, a supplier or an affiliate); or

- The Processing is necessary to comply with the organisation's legal obligations or exercise legal rights; or
- The Processing is required for a task in the public interest, or in the exercise of the organisation's official authority;
- The Processing is in the organisation's legitimate interests and does not unduly prejudice the individual's privacy.

5.5 That, to the extent that the Organisation Processes Special Categories of Personal Data, it must ensure that such Processing satisfies the conditions for Processing required by the Data Protection and Privacy Laws.

5.6 IIDC will publish privacy notices in respect of its processing of Personal Data of staff, suppliers, partners and visitors, which tell those people what data is collected about them, what it is used for, the legal basis for Processing the data, who it will be shared with and how long it will be held for. When gathering Personal Data or establishing new data protection activities, members of staff should check existing privacy notices to see whether they need to be updated to reflect the new activities, or whether new privacy notices are required to cover that activity. They should also ensure that any new Processing activities are added to the organisation's Record of Processing Activities.

5.7 There are limited exceptions to the requirement to give Data Subjects notice of processing activities. In any case of uncertainty as to whether a notification should be given or updated, staff should contact the Data Protection Officer In the event that staff Process Personal Data on behalf of another party (as a part of research activities or otherwise), due diligence should be carried out (and contractual protection obtained) to ensure appropriate data protection notices or consents have been given or obtained.

## 6. Compliance with the Policy

6.1 All employees or persons acting on behalf of IIDC have a responsibility to ensure compliance with this policy and the laws it is modelled after. It is the responsibility of employees in management and leadership to ensure that the decisions they make, and the way data is used in their areas, are in accordance with the guidelines in this document. In particular, the role of the data governance officer, data stewards, data custodians, data experts, data users and the data owners within each department is important as defined below.

6.2 In addition, particular designated roles have a larger responsibility in ensuring compliance as the work that they do entails heavy interaction with data. The roles related to interaction with data are listed below;

### 6.2.1 Data Controller

IIDC is the Data Controller in respect of Personal Data processed by and for IIDC.

### 6.2.2 Data Governance Officer [DGO]

This is the employee of IIDC in charge of ensuring that the Organization is compliant with this policy and the governing data laws. The Executive Director is the senior post holder and will have overall

responsibility for this policy. The DGO may also double as the Data Protection Officer (DPO) of the Organisation.

This DGO/DPO may be contacted at dataprotection@iidcug.org.

### 6.2.3 Data Custodian [DC]

For particular collection of data, the data custodian is the individual responsible for its storage security, availability, backup, access management, and other technical aspects to do with the storage of data. The data custodian provides the technical guidance and enforces the rules governing the data

### 6.2.4 Data Owner [DO]

The data owner is the senior manager responsible for the collection, maintenance and use of a specific dataset and its use. For this data, the functions for which the data is required are within the purview of the data owner.

### 6.2.5 Data Steward [DS]

This is the individual responsible for a particular data set on a day-to-day basis and ensures that the required data is collected, and that quality is maintained. He/she also sets the controls around this dataset.

### 6.2.6 Data Expert [DE]

An individual that has specialized skills to work with data even though they may not be responsible for any dataset from a technical, functional or business point of view but possess. These include data analysts, data scientists among others.

### 6.2.7 User

A user is anyone that makes use of data in their work.

### 6.2.8 Information Management Group (IMG)

An Information Management Group (IMG) shall be established to define, advise, steer and monitor Information Management (including in relation to data protection) within IIDC. This includes overseeing information management roles and responsibilities, policies and procedures and activities in order to embed compliance, promote best practice, and provide technical solutions within all Departments and programs. The Information Management Group shall be constituted by the following; the Head of Programmes, The Finance and Administration Manager, The TA Monitoring and Evaluation, The Data Protection Officer, IT Officer

### 6.2.9 Role of Head of Departments, Program coordinators and Heads of programs

These persons have an overall responsibility for the Processing of Personal Data within their own departments or Programs and for ensuring that such Processing is undertaken in a way that is compliant with this policy.

All those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within IIDC, but ultimately, compliance with data protection legislation is the responsibility of all members of the organization who Process Personal Data.

### 6.2.10 Role of Staff of the Organisation

6.2.10.1 All staff are responsible for:

a) Ensuring that they have undertaken organization-provided data protection training;
b) Checking that any information that they provide the organization in connection with their employment is accurate and up to date and for informing the organization of any changes to their personal data (e.g. change of address); and
c) Ensuring that any Personal Data Processed by them is Processed in accordance with the Data Protection and privacy Laws and with this policy.

6.2.10.2 Staff procuring cloud-based services or mobile apps storing personal data for the organisation must check with the Cyber security and Risk Manager that these meet the security requirements of Data Protection legislation.

6.2.10.3 All staff are responsible for checking that any information they provide the organization in connection with their employment and stay at the organization is accurate and up to date and for informing the organization of any changes to their Personal Data (e.g. change of address).

6.2.10.4 Staff should not conduct profiling exercises without first conducting a data protection impact assessment. Should they accidently through manipulation of data sets find they have identified individuals, they should contact the Data Protection Officer/DGO. Profiling is defined as 'any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her'.

## 7. The Rights of Data Subjects

7.1 Under the Data Protection and Privacy Laws, Data Subjects have the following rights regarding the Processing of their personal date. They include;

a) The right to be informed about the purpose for the collection of their data.
b) The right of access to personal data held by the organisation about them (please see Clause 22);
c) The right to rectification of any inaccurate personal data held by the Organisation about them. (See Clause 24)

d) The right to erasure (also known as the 'right to be forgotten'); This right of erasure will only apply where, for example, the organisation no longer needs to use the Personal Data to achieve the purpose it collected it for; or where the Data Subject withdraws their consent if the organisation is using their Personal Data based on Data Subject consent; or where the Data Subject objects to the way the organisation Processes their data and this is upheld; (See clause 26)

e) The right to restrict processing of their personal data. This right will only apply where, for example, the Data Subject disputes the accuracy of the Personal Data the organsiation holds; or where they would have the right to require the organisation to erase the Personal Data but would prefer that its Processing is restricted instead; or where the organisation no longer needs to use the Personal Data to achieve the purpose for which it was collected, but it requires the data for the purposes of dealing with legal claims. In cases where the organisation has disclosed data to another party, and it is not disproportionate for the organisation to do so, it will let the recipients of the data know that the organisation has rectified, erased or restricted its Processing of it;

f) The right to data portability. Data Subjects also have the right to transfer (or require the organization to transfer) this Personal Data to another organisation (for example, a new employer or partner); (See Clause 28)

g) The right to object to the organisation's Processing of Personal Data it holds about them (where its justification for Processing the data is either that the Processing is necessary for the performance of a task in the public interest, or for the purposes of its own legitimate interests);

h) Rights with respect to automated decision-making and profiling. (See Clause 30)

i) Right to require a review. Data Subjects may ask the organisation to review any decisions that it has made about them using automated Processing.

j) Right to withdraw their consent, where the organisation is relying on it to Process their personal data.

k) Right to prevent the Processing for the purposes of direct marketing; (See Clause 32)

7.2 The organisation will have procedures in place to ensure that these rights can be exercised and will officially publicize them.

7.3 If staff or partners have concerns about the way in which their personal data is being used or Processed by the organisation, they may contact the Data Steward (DS) /Data Custodian (DC), in the first instance. If after this, they are not satisfied they can escalate their concern to the Executive Director (DGO/DPO) and if they are not satisfied by the organisation's response they have the right to lodge a formal complaint with the PDPA Data protection Officer.

## 8. Disclosure of Personal Data

8.1 IIDC shall ensure that Personal Data is not disclosed to unauthorized third parties. This includes family members, friends, government bodies, the media, and in certain circumstances, the Police.

8.2 All staff and partners of IIDC should exercise caution when asked to disclose Personal Data held by the organization about another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually

be appropriate to disclose a colleague's personal details to someone who wished to contact them regarding a non-work-related matter, especially when such details are not otherwise publicly available (such as work contact details on the organisation's website). The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of organization business.

8.3 This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

a) Where the disclosure is in the legitimate interests of the organization (e.g. disclosure to staff – Personal Data can be disclosed to other organization employees if it is clear that those members of staff require the information to enable them to perform their jobs);
b) Where the organisation is legally obliged to disclose the data or
c) Where disclosure of data is required for the performance of a contract (e.g. informing a supplier of changes in contract pricing etc.).

8.4 If Personal Data is to be shared with a third party in connection with the performance of a contract, then approved data protection clauses must be included in the relevant contract. IIDC's Data Protection Officer should be consulted on every occasion before any such contracts are entered into and Personal Data must not be shared with the third party until an appropriate contract is in place.

8.5 The Data Protection and privacy Laws permit certain disclosures without notification to the Data Subject in certain cases, so long as the information is requested for one or more of the following purposes:

a) to safeguard national security
b) prevention or detection of crime including the apprehension or prosecution of offenders;
c) assessment or collection of tax duty;
d) discharge of regulatory functions (includes health, safety and welfare of persons at work);
e) to prevent serious harm to a third party; or
f) to protect the vital interests of the individual; this refers to life and death situations.

8.6 Requests must be supported by appropriate paperwork and should follow the agreed protocols if in place. Where a third-party request is received citing one of these grounds, the request should be passed to an authorised person within the organisation for approval before any information is related. The authorised personnel is the Executive Director (the DPO/DGO) are, the Data Protection Officer/Data Steward, and the Executive Director of IIDC.

8.7 When members of staff receive enquiries as to whether a named individual is a member of the organisation (staff or supplier), the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the organisation may constitute an unauthorised disclosure of Personal Data.

8.8 Unless the Data Subject has requested otherwise, Personal Data should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the Data Subject consenting to disclosure to the third party should accompany the request.

8.9 As an alternative to disclosing Personal Data, the staff member/representative may offer to do one of the following:

- Pass a message to the Data Subject asking them to contact the enquirer; or
- accept a sealed envelope/incoming email message and attempt to forward it to the Data Subject.

- Inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the organisation" to avoid confirming their membership of, their presence in or their absence from the organisation.
- If in doubt, staff should seek advice from their line manager or Data Protection Officer/Data Steward/Data Governance Officer.

## 9. Adequate, Relevant, and Limited Data Processing.

9.1 IIDC will only use or process relevant and necessary data, and only when it is necessary to do so. IIDC will not process data in excess of the limit prescribed by law or required for the purpose for which the data is sought to be processed.

9.2 IIDC will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed.

9.3 IIDC will stop processing data of a data subject as soon as the need to do so has ceased.

## 10. Transparency and Participation.

10.1 IIDC shall ensure that the processing of personal data is transparent and enables for the participation of data subjects, include to provide consent, request for information on the personal data collected and request for correction of personal data.

10.2 IIDC shall ensure that:

a) Data subjects are aware of the nature and category personal data collected;
b) Whether or not the provision of the data by the data subject is mandatory or optional;
c) Data subjects are aware of the consequences for failure to provide the data, if any;
d) The authorisation requirement for the collection of the data [such as a legal, regulatory or contractual requirement] is acquired/obtained.
e) The recipients of the data, if the data is to provided or made accessible to third parties.
f) That there is in existence a right to access the data and the right to request rectification of the data;
g) Data subjects are aware of the purposes of the collection of the data;
h) Data subjects are aware of the expected duration for its processing.

## 11. Lawful and Fair Data Processing

11.1 IIDC shall ensure that the personal data is collected and processed in a manner that fair and lawful.

11.2 IIDC shall ensure that:

a) There shall be no collection or processing of special personal data except in compliance with a legal obligation, or with the employee's consent or in the circumstances permitted by law;
b) Where the data is collected or processed for different unrelated purposes, the data subject has consented to the collection or processing for each purpose, except if the same consent is reasonably clearly implied;

c) The processing is necessary for the purposes of the legitimate interests pursued by the IIDC or by a third party.

## 12. Specified, Explicit, and Legitimate Purposes for collection of personal data

12.1 IIDC collects and processes the personal data of a data subject for specified, explicit, and legitimate purposes.

12.2 IIDC only collects, processes, and holds personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by the law).

12.3 Data subjects shall be kept informed at all times of the purpose or purposes for which IIDC uses their personal data.

## 13. Accuracy of Data and Keeping Data Up-to-Date.

13.1 IIDC shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data.

13.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken to amend or erase that data, as appropriate.

## 14. Consent

14.1 Subject to this policy, and to the law, the personal data of any data subject shall not be collected or processed by IIDC without their express, unequivocal, prior and informed consent to the collection or processing of their personal data.

14.2 IIDC shall clearly inform data subjects of the intention to collect or process data, the purpose for use or collection of the data, the mode of processing of that data, the expected period of retention or processing of that data, the rights of data subjects as well as any other information that shall be reasonably necessary to provide data subjects with sufficient information to make an informed decision.

14.3 IIDC's DGO or their designate shall receive and reasonably promptly respond to all queries regarding the collection, use, processing or storage of the personal data of data subjects.

## 15. Keeping Data Subjects Informed

15.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

15.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) If the personal data is used to communicate with the data subject, when the first communication is made; or

b) If the personal data is to be transferred to another party, before that transfer is made; or

c) As soon as reasonably possible and in any event not more than one month after the personal data is obtained.

15.3 The following information shall be provided:

a) Details of IIDC including, but not limited to, the identity of its DGO;
b) The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
c) Where applicable, the legitimate interests upon which IIDC is justifying its collection and processing of the personal data;
d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
e) Where the personal data is to be transferred to one or more third parties, details of those parties;
f) Details of data retention;
g) Details of the data subject's rights;
h) Details of the data subject's right to withdraw their consent to IIDC's processing of their personal data at any time;
i) Details of the data subject's right to complain to the Data Protection Office;
j) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
k) Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

## 16. Processing of Special Personal Data.

16.1 Special Personal Data of a data subject is afforded a higher level of protection by law. It will normally be necessary to have an individual's explicit consent to Process such data.

16.2 IIDC shall not participate in the collection or processing of special personal data of a data subject (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), except if at least one of the following conditions is met:

a) Personal data is collected or processed with the prior consent of the employee, except where such data is required to be collected or processed by virtue of a legal obligation, for public purposes [such as for national security, detection or prevention of a crime or the discharge of public functions], contractual obligations which applies to the data subject, for medical purposes or compliance with a legal obligation to which applies to the data subject;
b) The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law;
c) The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) The processing relates to personal data which is clearly made public by the data subject;
e) The processing is necessary for the conduct or investigation of legal claims arising out of some judicial processing; or
f) The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in law;

## 17. Collection of Personal Data.

17.1 Personal data is only collected to meet a particular purpose and with the intention to use it for that purpose only.

17.2 All persons whose data is collected must provide explicit consent to the collection of their data and must be made aware of the purpose for which it is collected.

17.3 Persons collecting data should ensure that the integrity of the data is maintained during collection and that it is not altered in any way that changes how it is interpreted.

17.4 During collection, data should not be adjusted, amended or altered by means of adding extra information, removing bits of information or adjusting them in ways that differ from what was recorded directly.

## 18. Secure Processing of Data /Security of Data.

18.1 IIDC shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

18.2 IIDC shall ensure that all personal data collected, held or processed is stored in Uganda or in a country with, at least, the same data protection laws and standards as Uganda.

18.3 All staff are responsible for ensuring that any Personal Data (on others) which they hold is kept securely in line with the organisation's Data Security Policy and Procedure and in appropriate systems and that such data is not disclosed to any unauthorised third party.

18.4 All Personal Data should be accessible only to those who need to use it. A judgment should be made based upon the sensitivity and value of the information in question, but consideration should always be given to keeping Personal Data:

a) in a lockable room with controlled access;

b) in a locked drawer or filing cabinet; or

c) if computerised, password protected.

18.5 Personal Data must not be stored on removable media (such as USB storage devices, removable hard drives, CDs or DVDs) or mobile devices (laptops, tablets or smart phones) unless it is encrypted or password protected, and the key kept securely. A backup copy should also be kept on the secure organisation servers. Personal Data must not be stored in generic personal cloud services such as Dropbox.

18.6 Extreme care should be taken when sending emails that contain Personal Data. General guidance on the use of email is available from the Organisation's IT Policy.

18.7 If Personal Data is transferred using removable media, a secure, tracked service must be used to ensure safe delivery.

18.8 Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised individuals.

18.9 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of Personal Data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be securely wiped clean before disposal. If in doubt as to what the correct security measures are for the deletion or disposal of Personal Data, advice should be taken from IT and data Protection Officers. .

18.10 Where the organization uses external organisations to Process Personal Data on its behalf additional security arrangements will be implemented in contracts with those organisations to safeguard the security of Personal Data. Mandatory legal protections will always be included in any contract with such parties. Any Data Processing agreement the organization enters into must contain such protections.

18.11 In the event that the organization acts as a Data Processor (please see below), Processing personal data on behalf of a third party, such third party may require additional security arrangements to be implemented. Mandatory legal protections will be included in the contract, and will be flowed-down to any sub-processor used by the organisation.

18.12 Members of IIDC should consult their line manager or the Data Protection Team to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

## 19. Acting as a Data Processor

19.1 When IIDC Processes the Personal data of staff, suppliers, contractors, partners and other individuals (in a professional or personal context) it is ordinarily the case that the organization would be known as a Data Controller.

19.2 A Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, Processed.

19.3 In some limited circumstances, IIDC may be a Data Processor; i.e. it is Processing the data on behalf of a third-party Data Controller.

19.4 If Members of IIDC are handling Personal Data and are not sure whether the organisation is acting as a Data Controller or a Data Processor, they should contact their line manager, Data Protection Officer or the Data Protection Team in the first instance. It is key to understand the relationship, in order to determine how such personal information should be handled.

19.5 The Data Controller has the majority of the obligations under the Data Protection and privacy Laws, e.g. in respect of Data Subject rights and ensuring appropriate consents are obtained or privacy notices are given.

19.6 However, a Data Processor also has a number of obligations under Data Protection and privacy Laws. In most cases, the Processing obligations imposed on the organization will be guided by the contract entered into between the organization and the third party on whose behalf it is Processing.

## 20. Accountability and Record-Keeping

20.1 IIDC shall have a Data Governance Officer ["DGO"] whose role is to ensure compliance with data protection laws, regulations and best practices. The name and details of the DGO are included to this policy as Annex I. The DGO shall execute all be the equivalent of a Data Protection Officer under the Data Protection and Privacy Act and discharge the mandate of that officer in respect of IIDC.

20.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, IIDC's other data protection-related policies and other applicable data protection legislation.

20.3 IIDC shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of any applicable third-party data processors;
b) The purposes for which IIDC collects, holds, and processes personal data;
c) Details of the categories of personal data collected, held, and processed by IIDC, and the categories of data subject to which that personal data relates;
d) Details of how long personal data will be retained by IIDC; and
e) Detailed descriptions of all technical and organisational measures taken by IIDC to ensure the security of personal data.

## 21. Data Protection Impact Assessments

21.1 IIDC shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data where the collection or processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects.

21.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

a) The type(s) of personal data that will be collected, held, and processed;
b) How the personal data is intended to be collected or processed;]
c) The purpose(s) for which personal data is to be used;
d) How personal data is to be used;
e) The parties (internal and/or external) who are to be consulted;
f) The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
g) Risks posed to data subjects;
h) Risks posed both within and to IIDC; and
i) Proposed measures to minimise and handle identified risks.
j) Any other matters required to be addressed by the Personal Data Protection Office ["PDPO"].

## 22. Data Subject Access to personal data

22.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which IIDC holds about them, what it is doing with that personal data, and why.

22.2 Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to IIDC's DGO at the email address indicated in Annex I or by physically tendering in the SAR Form to the DGO.

22.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

22.4 All SARs received shall be handled by IIDC's DGO, except that the officers indicated in Annex II may handle a SAR on the direction of management.

22.5 IIDC does not charge a fee for the handling of normal SARs. IIDC reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

## 23. Third Party access to data

In addition to the above, where the organization is acting as a Data Processor, it will have a responsibility to provide assistance to the third party it is Processing Personal Data on behalf of, in respect of individuals exercising their rights.

The contract between the organization and the third party it is Processing Personal Data on behalf of, may also have additional contractual restrictions or timescales in respect of such support/ assistance. You should check the contractual position carefully prior to (a) responding to a request made directly by an individual or third party, or (b) providing assistance to the third party; and check with the Data Protection Team if you are unclear how to proceed.

## 24. Rectification of Personal Data

24.1 Data subjects have the right to require IIDC to rectify any of their personal data that is inaccurate or incomplete.

24.2 IIDC shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing IIDC of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

24.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

## 25. Retention and Disposal of Data

25.1 IIDC shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

25.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it.

25.3 IIDC discourages the retention of Personal Data for longer than it is required.

25.4 IIDC aims to reduce the duplication of personal data and will encourage as far as possible the use of definitive central sources of information for data used across the organisation (e.g. contact addresses). Those with legitimate reason will have access to the Personal Data relevant for their job. Permissions granted for such access will be logged where possible and regularly reviewed.

25.5 The creation of systems and/or files which duplicate such data should be avoided; where it is inevitable every care should be taken to ensure that data maintained in subsidiary systems is fully synchronized with definitive sources, and updated frequently through secure and reliable interconnection.

**Suppliers**

25.6 In general, electronic supplier records maintained in the Organisation are kept permanently in order to fulfil the requirement for the provision of services during a supplier's or former supplier's contractual/working life. Such information would typically include name and address on entry and completion, services/products provided among others.

25.7 Departments and programs shall regularly review the personal files that they hold relating to individual suppliers (whether stored electronically or in paper records) in accordance with the organisation's Retention and Disposal Schedule.

**Partners**

25.8 Electronic partner records maintained in the Organisation are kept permanently in order to fulfil the requirement for the provision of services during a partner's contractual/working life. Such information would typically include name and address on entry and completion, services/products provided among others.

25.9 Departments and programs should regularly review the personal files that they hold relating to each partner (whether stored electronically or in paper records) in accordance with the organisation's Retention and Disposal Schedule.

**Staff**

25.10 In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by Human Resources for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay, etc. will be retained for the statutory time period (between 3 and 6 years).

25.11 Staff Human Resources records are kept and maintained by Human Resources. Other departments should only keep staff information where necessary for legitimate business purposes.

25.12 Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for six months from the interview date and should then be securely destroyed as confidential waste. Human Resources may keep a record of names of individuals that have applied, been short-listed, or interviewed, for posts indefinitely.

25.13 This is to aid management of the recruitment process.

**Disposal of Records**

25.14 Personal Data must be disposed of in a way that protects the rights and privacy of Data Subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion) and in line with the organisation's Retention and Disposal Schedule.

## 26. Erasure of Personal Data

26.1 Data subjects have the right to request that IIDC erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for IIDC to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
b) The data subject wishes to withdraw their consent to IIDC holding and processing their personal data;
c) The data subject objects to IIDC holding and processing their personal data (and there is no overriding legitimate interest to allow IIDC to continue doing so);
d) The personal data has been processed unlawfully;
e) The personal data needs to be erased in order for IIDC to comply with a particular legal obligation.

26.2 Unless IIDC has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

26.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

## 27. Restriction of Personal Data Processing

27.1 Data subjects may request that IIDC ceases processing the personal data it holds about them. If a data subject makes such a request, IIDC shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

27.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

## 28. Automations and Data Portability

28.1 Where data subjects have given their consent to IIDC to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between

IIDC and the data subject, or by law, data subjects have the right, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

28.2 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

28.3 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

## 29. Objections to Personal Data Processing

29.1 Data subjects have the right to object to IIDC processing their personal data.

29.2 Where a data subject objects to IIDC processing their personal data based on its legitimate interests, IIDC shall cease such processing immediately, unless it can be demonstrated that IIDC's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is permitted by law.

## 30. Automated Decision-Making

30.1 IIDC may use personal data in automated decision-making processes. A data subject shall have the right to obtain, from the DGO, details on how an automated process uses personal data to arrive at a decision.

30.2 Where such decisions have a significant effect on data subjects, those data subjects have the right to challenge to such decisions, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from IIDC.

30.3 The right described in Clause 15.2 does not apply in the following circumstances:

a) The decision is necessary for the entry into, or performance of, a contract between IIDC and the data subject;
b) The decision is authorised by law; or
c) The data subject has given their explicit consent.

## 31. Profiling

31.1 IIDC may use personal data for profiling purposes. This will largely be for reporting or management use, such as to track IIDC's diversity and inclusiveness.

31.2 When personal data is used for profiling purposes, the following shall apply:

a) Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;
b) Appropriate mathematical or statistical procedures shall be used;
c) Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

## 32. Direct Marketing

32.1 Any proposal to carry out direct marketing (i.e. marketing by email, telephone, post or any other means that is directed at a particular individual, whether they are a staff, supplier, partner or otherwise) must be reviewed and approved in advance by the organisation Data Governance Officer .

32.2 Members of IIDC should not send direct marketing material to someone electronically (e.g. by email, Whatsapp, social media messenger services or targeted banner ads) unless there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their Personal Data for direct marketing purposes and should notify the relevant marketing team about any such request.

32.1 Any Department or Program that uses Personal Data for direct marketing purposes must inform Data Subjects of this at the time of collection of the relevant Personal Data and may only make direct marketing communications where the Data Subject has opted-in to receiving such communications. Data Subjects must also be given the opportunity to opt out of receiving communications at any time and measures must be put in place to prevent such communications from being sent once the Organisation has received confirmation that a Data Subject has opted out.

## 33. Personal Data Collected, Held, and Processed

a) The following personal data is collected, held, and processed by IIDC:

| Data Ref. | Type of Data | Purpose of Data |
|---|---|---|
| 1 | Name | To attach to Personal file |
| 2 | Nationality | To attach to Personal file |
| 3 | Age | To attach to Personal file |
| 4 | Marital status | To attach to Personal file |
| 5 | Postal address | Address information |
| 6 | Bank account name and number | To attach to Personal file and to make payments |
| 7 | Date of birth | To attach to Personal file |
| 8 | Email address | For communication purposes |
| 9 | Drivers license or passport number | To attach to Personal file |
| 10 | Social security number | To attach to Personal file and make payments |

## 34. Data Security - Transferring Personal Data and Communications

34.1 IIDC shall, as far as possible, ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

(a) All emails containing personal data must be encrypted;

(b) All emails containing personal data must be marked "confidential";

(c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

(d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

(e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

(f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

(g) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient; and

(h) All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

## 35. Data Security - Storage

35.1 IIDC shall ensure that the following measures are taken with respect to the storage of personal data:

35.1.1 All electronic copies of personal data should be stored securely using passwords and data encryption;

35.1.2 Systems that provide access to data should enforce a two-factor authentication mechanism;

35.1.3 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

35.1.4 All personal data stored electronically should be backed up regularly. Backups may be stored onsite and/or offsite. All backups should include encryption and authentication;

35.1.5 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to IIDC or otherwise [without the formal written approval of the DGO and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary]; and

35.1.6 No personal data should be transferred to any device personally belonging to an employee

and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of IIDC where the party in question has agreed to comply fully with the letter and spirit of this Policy (which may include demonstrating to IIDC that all suitable technical and organisational measures have been taken).

## 36. Data Security - Disposal

36.1 When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

## 37. Data Security - Use of Personal Data

37.1 IIDC shall ensure that the following measures are taken with respect to the use of personal data:

37.1.1 No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of IIDC requires access to any personal data that they do not already have access to, such access should be formally requested from the DGO;

37.1.2 Access rights should be clearly defined by the data owner ensuring that users do not have more access than they need to perform their roles, and these should be approved by the DGO. The access right definitions must be documented in a data governance document for any system or project. This document will be required for signoff from the DGO before a system or project can be deployed.

37.1.3 No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of IIDC or not, without the authorisation of the DGO;

37.1.4 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

37.1.5 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

37.1.6 Where personal data held by IIDC is used for marketing purposes, it shall be the responsibility of DGO to ensure that the appropriate consent is obtained and that no data subjects have opted out, except where such consent has been given whether expressly or implicitly.

## 38. Data Security - IT Security

38.1 IIDC shall ensure that the following measures are taken with respect to IT and information security:

38.1.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. [All software used by IIDC is designed to require such passwords.];

38.1.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of IIDC, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable

method. IT staff do not have access to passwords;

38.1.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. IIDC's IT staff shall be responsible for installing any and all security-related updates; and

38.1.4 No software may be installed on any Company-owned computer or device without the prior approval of the DGO or IT Manager.

## 39. Publication of Organisation Information.

39.1 IIDC publishes particular information that include Personal Data, and will continue to do so. Some of this information includes;

a) names of all staff members of the organisation and names of partner organisations;
b) staff profiles on the organisation website, including names, job titles and photographs;
c) Staff Telephone and Email Directory;
d) Events and videos or other multimedia versions of events ;
e) information in prospectuses (including photographs), annual reports, staff newsletters, etc.;
f) publicity information included in public relations stories and press releases and on social media; and
g) staff information on the organisation website (including photographs).

39.2 It is recognized that there might be occasions when a member of staff, a partner, or other party, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the Organisation should use its reasonable endeavors to comply with the request and ensure that appropriate action is taken.

## 40. General Organisational Guidelines with respect to collection, holding and processing of personal data.

40.1 IIDC shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

40.1.1 All employees, agents, contractors, partners, or other parties working on behalf of IIDC shall be made fully aware of both their individual responsibilities and IIDC's responsibilities under the law and under this Policy, and shall be provided with a copy of this Policy;

40.1.2 Only employees, agents, sub-contractors, or other parties working on behalf of IIDC that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by IIDC;

40.1.3 All employees, agents, contractors, or other parties working on behalf of IIDC handling personal data will be appropriately trained to do so;

40.1.4 All employees, agents, contractors, or other parties working on behalf of IIDC handling

personal data will be appropriately supervised;

40.1.5 All employees, agents, contractors, or other parties working on behalf of IIDC handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

40.1.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

40.1.7 All personal data held by IIDC shall be reviewed periodically;

40.1.8 The performance of those employees, agents, contractors, or other parties working on behalf of IIDC handling personal data shall be regularly evaluated and reviewed;

40.1.9 All employees, agents, contractors, or other parties working on behalf of IIDC handling personal data will be bound to do so in accordance with the principles of the DPPA and this Policy by contract;

40.1.10 All agents, contractors, or other parties working on behalf of IIDC handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of IIDC arising out of this Policy and the law; and

40.1.11 Where any agent, contractor or other party working on behalf of IIDC handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless IIDC against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

## 41. Transferring Personal Data to a Country Outside Uganda.

41.1 IIDC may from time-to-time transfer ('transfer' includes making available remotely and storing) personal data to countries outside of Uganda as provided in the Data Protection and Privacy Act, 2019.

41.2 The transfer of personal data to a country outside of Uganda shall take place only if one or more of the following applies:

41.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that Uganda has determined ensures an adequate level of protection for personal data;

41.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards akin to those provided under Ugandan law;

41.2.3 The transfer is necessary for the performance of a contract between the data subject and IIDC (or for pre-contractual steps taken at the request of the data subject);

41.2.4 The transfer is necessary for important public interest reasons;

41.2.5 The transfer is necessary for the conduct of legal claims; or

41.2.6 The transfer is necessary to protect the vital interests of the data subject or IIDC or other individuals where the data subject is physically or legally unable to give their consent.

## 42. Data Breach Notification

42.1 All personal data breaches must be reported immediately to IIDC's DGO.

42.2 All personnel and staff of IIDC have an obligation to report actual or potential data protection compliance failures to the Data Governance Officer/Data Protection Officer immediately they become aware of them, following the published breach notification procedure.

42.3 The Data Protection and privacy Laws provide that breaches must be notified to the Data Protection Officer as soon as possible and in any event within 72 hours of becoming aware of them

42.4 The DGO shall ensure, as soon as possible, that the PDPO is made aware of the data breach, and shall affect the directions of the PDPO including to inform the data subject if so directed.

42.5 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the DGO shall seek guidance from the PDPO, and effect its directions without undue delay.

42.6 Data breach notifications shall include the following information:

42.6.1 The categories and approximate number of data subjects concerned;

42.6.2 The categories and approximate number of personal data records concerned;

42.6.3 The name and contact details of IIDC's data protection officer (or other contact point where more information can be obtained);

42.6.4 The likely consequences of the breach;

42.6.5 Details of the measures taken, or proposed to be taken, by IIDC to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

42.7 Where IIDC is acting as a Data Processor, it will have a responsibility to notify actual or potential data protection compliance failures to the third party it is Processing personal data on behalf of. The contract between the organization and the third party it is Processing personal data on behalf of may also have additional contractual restrictions or timescales in respect of such support/ assistance. Members of the organization should check the contractual position carefully and check with the DPO/DGO if they are unclear how to proceed.

## 43. Further Information

43.1 Useful web addresses:

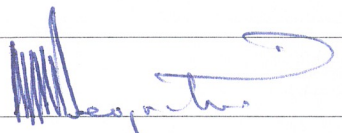
https://www.pdpo.go.ug/home

43.2 For further guidance or advice on the Data Protection and privacy Laws or this policy and its application, please contact Organisation Data Protection Officer by email at dataprotection@iidcug.org

## 44. Implementation of Policy

44.1 This Policy shall be deemed effective as of 1st June 2023. No part of

this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

| POLICY SIGN-OFF AND OWNERSHIP DETAILS | |
|---|---|
| **Document name:** | Data Protection Policy |
| **Version Number:** | 1.0 |
| **Approved by:** |  |
| **Date Approved:** | 20.06.2023 |
| **Next Review required by:** | 20.06.2026 |
| **Author:** | IIDC |
| **Owner (if different from above):** | IIDC |
| **Compliance Checks:** | |
| **Related Policies/Procedures:** | IIDC IT policy |

| REVISION HISTORY |
|---|

| Version | Date | Revision description/Summary of changes | Author |
|---|---|---|---|
| | | | |
| | | | |

**Annex I: Name and Details Of DGO**

**(Insert name)**

**Annex II: Officers of IIDC Who May Handle SAR On Direction of Management**

**(Insert names)**