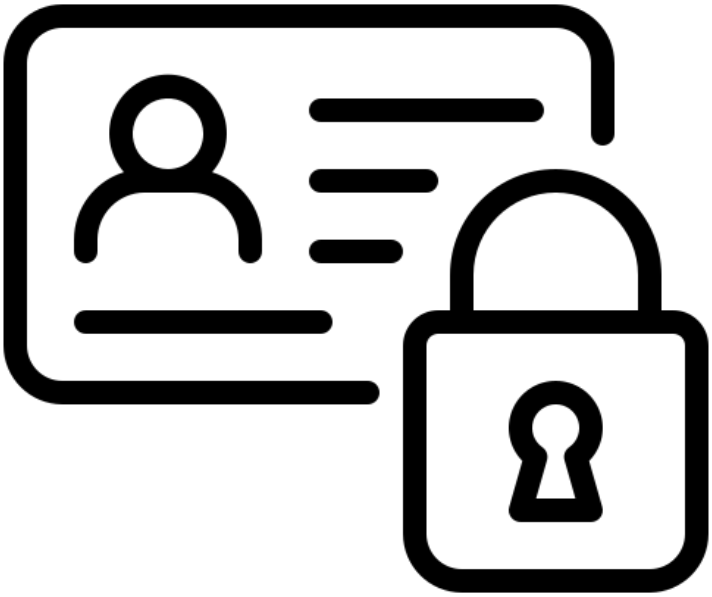

DATA PROTECTION POLICY

(2023-2024)

VERSION 1.0

(DRAFT PENDING FOR APPROVAL FROM BOARD)

Conference of Religious Women, India

C/O Apostolic Carmel Generalate,# 06, East end road, Jayanagar 4th Block, Jayanagar East, Bangalore, Karnataka 560041

DISCLAIMER, CREDITS

This policy has been framed keeping in mind the ethical considerations to be made while collecting and processing personal data, legal compliances to be followed as well as maintaining privacy of individuals and safeguarding against vulnerability related to data and its misuse in the current scenario.

As an organization, CRWI is committed to comply with the international standards and National policies and laws governing organizations and staff within the organization while managing and working with people and using information related to people.

Few sources and documents, internally and externally, were referred to during the construction of this policy. We, at CRWI, extend our gratitude and thanks to all those sources and documents which helped us give shape to this document to be implemented in the organization for building trust, transparency, and integrity.

CONTENTS

1 CHAPTER ONE-GENERAL

1.1 BACKGROUND

1.1.1 Since its inception, CRWI has been implementing projects and initiatives with households or institutions and in the process, there has been exchange of information between the two entities to accommodate transfer of knowledge, skills and resources. In this process of exchange of information varied data is collected as a necessity from these participants to ensure the right participant at the right time and for rightful purpose receives support or benefits which enhances their living and life.

1.1.2 During these transfers, many such data are collected to comply with the intervention, law, and donors to maintain transparency and compliances, track changes, and gauge impact. This data could be contextual to individual, community, or institutions, sensitive or generic in nature, implications could be non or grave.

1.2 WHAT IS DATA PRIVACY

1.2.1 Data privacy in general terms means the ability of any individual or collectives to determine for themselves or for their families/ communities or institutions when, how, and to what extent personal information about them is shared with or communicated to others. This personal information can be one's name, location, contact information, or online or real-world behavior. For e.g. someone may exclude themselves from sharing information in a direct dialogue or conversation while seeking information, or many people may have control and prevent certain personal data disclosure when sought online or virtually.

1.3 WHY DATA PRIVACY

1.3.1 In many jurisdictions and countries, privacy is a fundamental human right, and data protection laws exist to guard that right. Data privacy is also important because the person agreeing and willing to engage online, they must trust that their personal data will be handled with care. Organizations use data protection practices to demonstrate to other stakeholders and users that they can be trusted with their personal data.

1.3.2 Personal data can be misused in numerous ways if it is not kept private, safe and protected or if whose data is being collected don't have the knowledge and ability to control how their information is used:

- Personal data to defraud or harass individual.
- Entities may sell personal data to others for profits.
- May restrict their ability to express themselves freely.
- The outcomes can irreparably harm their reputation, as well as resulting in fines, sanctions, and other legal consequences.
- Many people and countries hold that privacy has intrinsic value: that privacy is a human right fundamental to a free society, like the right to free speech.

1.4 LAWS GOVERNING DATA PRIVACY

1.4.1 With the internet being integral part of life and as because technological advances have improved data collection and surveillance capabilities, many governments around the world have started passing laws regulating what kind of data can be collected about users, how that data can be used, and how data should be stored and protected. Some of the most important regulatory privacy frameworks to know include:

1.4.1.1 General Data Protection Regulation (GDPR): Regulates how the personal data of European Union (EU) data subjects, meaning , can be collected, stored, and processed, and gives data subjects rights to control their personal data (including a right to be forgotten).

1.4.1.2 THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023) [11th August 2023.] and THE DIGITAL PERSONAL DATA PROTECTION BILL, 2023: An Act to provide for the processing of digital personal data in a manner that recognizes both the right of to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

1.4.1.3 Apart from these are others Acts and laws specific to countries governing their citizens and the rights of the people in those countries. We are governed by the Indian laws and Acts.

1.5 WHAT WE UNDERSTAND BY DATA PROTECTION POLICY

1.5.1 Data protection Policy means strategic, procedural steps and Information security controls within the organization's working environment undertaken by CRWI to safeguard the privacy, availability, and integrity of sensitive data. These protective measures are critical for CRWI, which often collects, processes, or stores such sensitive data, with an aim to prevent data corruption, loss, or damage so that it is not only safeguarded but to ensure that it remains accessible and reliable, thus preserving trust and compliance and enhancing confidence/assurance to all stakeholders in data-centric operations.

1.6 SCOPE OF THIS POLICY

1.6.1 This policy sets out rules and governance structures related to protection of data of individuals, communities, institutions that CRWI works with, including its staff and applies to CRWI as an organization, its staff and any individual or entity working on its behalf, and all who provide personal data to CRWI.

1.6.2 The usage or processing of any Personal Data collected by the CRWI or and any individual or entity working on its behalf is subject to compliance with this Policy and any other relevant rules of the CRWI adopted for safeguarding data or data privacy.

1.6.3 The Data Protection Policy of CRWI will apply to the processing of digital personal data within India where such data is collected online, or collected offline and is digitized. It will also apply to such processing outside India, if it is for offering goods or services in India as per the Digital Data protection Bill 2023

1.7 PROPRIETORSHIP, MODIFICATION AND UPDATING OF POLICY

1.7.1 This Policy "Data Protection Policy" is the property of CRWI, meant for internal circulation & usage.

1.7.2 The Organization reserves the right to amend or modify this Policy in whole or in part, at any time in compliance with the National Law/s and Act's. The policy will be reviewed by the end of every Financial Year and if there are any amendments, it will be submitted to the Board for ratification and approval.

1.7.3 Any alteration, modification, change, addition or deletion will not be entertained until and unless done by the authorized person or designated person to do so by the Executive Director or the Board

1.7.4 This Policy will be shared for reference and use with all staff, irrespective of the level and responsibility and all entities that CRWI are engaged for carrying out the mission of CRWI.

2 CHAPTER TWO: PRINCIPLES

2.1 FAIRNESS AND LAWFULNESS

2.1.1 When processing personal data, the rights of an individual must be protected. Personal data must be collected and processed in a legal and fair and transparent manner in accordance with the existing laws and ethical considerations.

2.1.2 Individual data can be processed with voluntary consent of the person concerned.

2.2 LIMITATION AND RESTRICTION TO A SPECIFIC PURPOSE

2.2.1 Data collected should be contextual, adequate, relevant, and not excessive in relation to the purposes for which it is obtained.

2.2.2 Any personal data collected of an individual, community or an institution can be processed only for the purpose that was defined before the data was collected. Personal data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes. Subsequent changes to the purpose are only possible to a limited extent and require justification and administrative approvals.

2.2.3 However, further data processing for statistical, scientific, and historical purposes shall be considered compatible with the initial purposes of the data collection.

2.3 TRANSPARENCY

2.3.1 The individuals/ community/ institutions must be informed of how their data is being handled or would be handled. Personal data must be collected directly from the individual concerned and not from any other source. When the data is collected, the individuals/ community/ institutions must either be made aware of, or informed of:

- The purpose of data processing.
- Other parties to whom the data might be transmitted.

2.3.2 Processing of personal data must have received the consent of the individuals/ community/ institutions or must meet one of the following conditions: compliance with any legal obligation to which CRWI is subject to; the protection of the individuals/ community/ institution's life; the performance of a public service mission entrusted to CRWI.

2.4 CONFIDENTIALITY AND DATA SECURITY

2.4.1 All personal data is subject to complete data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

2.5 LIMITATION OF STORAGE AND DELETION

2.5.1 All Personal data shall be retained in a form that allows the identification of the individuals for a period no longer than necessary for the purposes for which it is obtained and processed. Once the purpose has been served, the data should be systematically and appropriately deleted from all the records.

2.6 FACTUAL ACCURACY AND UP-TO-DATEDNESS OF DATA

2.6.1 All Personal data collected must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented, or updated.

2.7 ACCOUNTABILITY TO DATA COLLECTED

2.7.1 CRWI will be responsible for all the data collected and will demonstrate compliance with the principles outlined above.

3 CHAPTER THREE: DEFINITIONS

3.1 PERSONAL DATA

3.1.1 Personal Data under Data Protection Policy means any information relating to an identified or identifiable individual/ Community/ Institution.

3.1.2 An identifiable individual/ Community/ Institution is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual or that of the community or an institution.

3.2 DATA PROCESSING

3.2.1 Data processing means any operation or a set of operations which is performed upon Personal Data or sets of Personal Data, by manual or automated means (including the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of Personal Data).

3.3 DATA CONTROLLER

3.3.1 This means any Staff Member or any authorized person on behalf of CRWI who has the authority to determine, alone or jointly with others, the purposes, conditions and means of the processing of Personal Data on behalf of the CRWI.

3.4 DATA PROCESSOR

3.4.1 Means any Staff Member or other individual, legal entity, public authority or similar body, including a third party, authorized to process Personal Data on behalf and under the direct authority of the Data Controller.

3.5 RECIPIENT

3.5.1 Recipient under Data Protection policy means the individual, legal entity, public authority, or similar body to which Personal Data are disclosed or shared.

3.6 PERSONAL DATA BREACH

3.6.1 This a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed which is done intentionally or unintentionally that brings harm to an individual/ community or institution.

3.7 SENSITIVE DATA

3.7.1 Sensitive data are those data related to or revealing sensitive information such as

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Subscriptions or memberships
- Physical or mental health
- Sex life
- Sexual orientation
- Criminal convictions, offences, or related security measures.
- Genetic data
- Biometric data

3.8 CONSENT

3.8.1 This means freely given, specific, informed, and unambiguous permission expressed by an individual, community or an institution by which they agree with the processing of their Personal Data.

3.8.2 This consent is given either by a written statement or by a clear affirmative action to the data collector.

3.8.3 CRWI will immediately stop any collection or processing of data if consent has been withdrawn either by verbal or through written statement anytime by the individual/ Community / Institution. No explanation for the withdrawal of consent will be asked for by the CRWI.

3.9 DATA PROTECTION OFFICER

3.9.1 Any staff member from the staff pool of CRWI appointed by the Executive Director or the Board to perform the duties listed in this Policy or assigned to him/her/them by decision of the Executive Director or the Board

3.10 STAFF

3.10.1 Means any staff member of the CRWI as defined in the HR policy of CRWI.

3.11 SUBJECT

3.11.1 Means all individuals whose data is being collected in the capacity of individuals/ community or institutions during execution of work of CRWI.

3.12 EXTERNAL ENTITY

3.12.1 All individuals / institutions engaged by CRWI in collection of Data and Processing of data on behalf of CRWI.

4 CHAPTER THREE: RIGHTS OF INDIVIDUALS

4.1 INFORMATION TO BE GIVEN TO THE INDIVIDUALS

4.1.1 On written or verbal request made by the concerned individual, CRWI shall provide the individual with the following information on the Processing of data which is personal to him/her/ them only:

- the identity and the contact details of the Data Controller
- the contact details of the Data Protection Officer
- the purpose of the Processing for which the personal data are intended as well as the legal basis for the processing.
- the categories of Personal Data concerned or being collected.
- the Recipients or category of Recipients of the Personal Data or the intended recipients and the use by them
- wherever possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the reason why no such period is fixed.
- wherever applicable, the fact that the CRWI intends to transfer Personal Data to a Member of the CRWI, another organization or a third party and the reasons for such transfer; and
- the existence of the right to request access, rectification, or erasure of Personal Data and to submit claims.

4.1.2 The section above shall not apply where the provision of such information proves impossible or would involve a disproportionate effort, and such impossibility or disproportionate effort is duly motivated by actions beyond the control of CRWI. In such instances, the CRWI shall take appropriate measures to protect the concerned individuals' rights and legitimate interests to the extent reasonably possible.

4.2 RIGHT TO ACCESS

4.2.1 Every individual shall have the right to obtain from the Data Controller at any time, on request, confirmation as to whether or not Personal Data relating to him/her/ them is being processed.

4.3 RIGHT TO RECTIFICATION AND ERASURE OF DATA

4.3.1 Subjects have the right to obtain, without undue delay, the rectification or completion of their inaccurate or incomplete Personal Data.

4.3.2 Subjects shall have the right to obtain from the Data Controller erasure of their Personal Data without undue delay, and the Data Controller shall have the obligation to erase Personal Data without undue delay where one of the following grounds applies:

- the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; or
- Personal Data has been processed in such a way that does not comply with this Policy.

4.3.3 Wherever the CRWI is not the Data Processor, CRWI shall make every reasonable effort to ensure that the External Data Processor complies with the request of the concerned individual/s.

4.3.4 The above section does not apply to the extent where processing is necessary for statistical or archiving purposes, for the delivery of the CRWI's mission of work, where erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing.

4.4 RIGHT TO RESTRICT PROCESSSING

4.4.1 Every individual shall have at any time the right to submit a request objecting, on grounds relating to his or her particular situation (to the email provided in the document), to the Processing of Personal Data concerning him or her or them. The Data Controller shall no longer process the personal data unless the Data Controller demonstrates that such Processing is necessary for the performance of the task carried out in the exercise of the CRWI official activities or in the framework of its missions.

4.5 RIGHT TO OBJECT

4.5.1 Unless CRWI has overriding compelling legitimate grounds for such Processing, Data Subjects may object to CRWI using their Personal Data for direct marketing purposes (including profiling) or for research or statistical purposes and may also object if CRWI is Processing their data on the grounds of pursuit of CRWI's legitimate interests.

4.6 RIGHT TO WITHDRAW CONSENT

4.6.1 If CRWI is relying on Consent as the basis on which CRWI is Processing a Data Subject's Personal Data, the Data Subject can withdraw their Consent at any time without any explanation.

4.7 RIGHT TO DATA PORTABILITY

4.7.1 Everyone shall have the right to receive the Personal Data concerning them, which they have provided to a Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Data Controller to which the Personal Data have been provided.

5 CHAPTER FIVE: DATA PROCESSING AND TRANSMISSION

5.1 LAWFULNESS AND FAIRNESS OF PROCESSING

5.1.1 Whenever Personal Data is Processed there must be one of the following legal bases present:

- the Data Subject has given his / her Consent.
- the Processing is necessary for the performance of a contract with the Data Subject
- to meet legal compliance obligations
- to protect the Data Subject's vital interests; or
- to pursue CRWI's legitimate interests such as implementation of projects and abiding by the agreed objectives of the projects in congruence to the law

5.2 CONSENT TO DATA PROCESSING

5.2.1 Personal data can be collected and processed upon consent of the person concerned of whose data is being collected. Declarations of consent must be submitted voluntarily. In certain exceptional circumstances, consent may be given verbally.

5.3 DATA PROCESSING PURSUANT TO LEGITIMATE INTEREST

5.3.1 Personal data can also be processed if it is necessary to pursue a legitimate interest of CRWI. Legitimate interests are generally of a legal (such as filing, enforcing, or defending against legal claims), audit or financial nature.

5.3.2 Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the individual merit protection. Before data is processed, it must be determined whether there are interests that merit protection or not.

5.3.3 Control measures that require processing of personal data can be taken only if there is a legal obligation to do so.

5.4 USE OF TELECOMMUNICATIONS AND INTERNET IN DATA PROCESSING

5.4.1 Telephone equipment, e-mail addresses, intranet, and internet along with internal social networks are provided by CRWI primarily for work-related assignments and organizational effectiveness. They are a tool and an organizational resource and can be used within the applicable legal regulations and internal CRWI IT and communication policies.

5.4.2 In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant IT laws must be observed if applicable.

5.4.3 There will be no general monitoring of telephone and e-mail communications or intranet/ internet use.

5.4.4 To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the network used by CRWI that block technically harmful content or that analyses the attack patterns.

5.4.5 For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be blocked for a temporary period. Evaluations of this data

from a specific person can be made only in some concrete, justified case of suspected violations of policies and/or procedures of CRWI.

5.4.6 The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the CRWI regulations.

5.4.7 All third-party platforms or software used for data collection and processing should have organizational clearance and legitimate with appropriate security measures and compliance.

5.4.8 Internal applications and platforms used for data collection and processing are to be timely updated and security measures enhanced.

5.5 TRANSMISSION OF PERSONAL DATA

5.5.1 Transmission of personal data to recipients outside or inside CRWI is subject to the authorization requirements from appropriate authority for processing personal data and requires the consent of the data subject. The data recipient must be required to use the data only for the defined purposes stated explicitly in the demand written and agreed.

5.5.2 Instances where data is transmitted to a recipient outside CRWI, this recipient must agree to maintain a data protection level equivalent to the CRWI Data Protection Policy. This does not apply if transmission is based on a legal obligation or demanded by the state under law.

5.5.3 If CRWI is using any external entity to Process Personal Data on CRWI's behalf, the Data Officer is responsible for ensuring that a GDPR compliant and Digital Personal Data Protection Act, 2023 contract is in place with the external entity and the external entity has agreed to adopt security measures to safeguard Personal Data that are appropriate to the associated risks.

5.5.4 If CRWI is Processing Personal Data jointly with an independent third party, CRWI must explicitly agree in the contract with that third party each party's respective responsibilities regarding Personal Data, signed and shared between both the parties.

5.5.5 Processing of personal data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the individual that merit protection must be taken into consideration.

5.5.6 Instances where, under legal obligation, to law enforcement agencies data are to be disclosed, the consent of the data subject is not necessary.

5.5.7 Only CRWI's Executive Director can validate any such disclosure in writing, ahead of the disclosure, after ensuring the request is legitimate, motivated by the requester, appropriate, necessary and does not pose a threat or direct risk to CRWI.

5.5.8 CRWI's Executive Director will check that the recipient of the data uses the data for the defined purposes only, and that it demonstrates the capacity and will to abide by such an obligation.

5.5.9 Wherever necessary, CRWI Executive Director will refer to legal advisers for advice, and to CRWI's Board for validation before transmitting personal data.

5.6 INFORMATION

5.6.1 CRWI as a committed organization, aims to ensure that individuals are aware that their personal data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights.

5.6.2 The current policy is shared with all CRWI staff and available on request by individuals. A version of this Policy is also available upon request to CRWI and made available on public domain.

5.6.3 The purpose of any action intended to provide access, by means of electronic transmission, to information previously stored in their electronic connection terminal device, or to record data in device shall be informed in a clear and comprehensive manner by CRWI to all subscriber or user of an electronic communication service.

5.7 CONFIDENTIALITY

5.7.1 As per the Data Protection Policy, Personal data is subject to data secrecy.

5.7.2 Unauthorized collection, processing, or use of such data by staff is prohibited.

5.7.3 Data processing undertaken by a staff that he/she/they have not been authorized to carry out as part of his/her legitimate duties is unauthorized and disciplinary actions are invited.

5.7.4 The "need to know" principle applies. Duly authorized staff may have access to personal information only as is appropriate for the type and scope of the task entrusted by the organization. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

5.7.5 Staff are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way.

5.7.6 Bring in a culture of data protection and privacy to adhere to protection laws and all staff should be made aware through training.

5.7.7 Supervisors must inform their team members at the start of the employment relationship about the obligation to protect data secrecy and accordingly mentioned in the appointment letter. *This obligation shall remain in force even after employment has ended pertaining to the personal data collected and processed during the tenure of service in CRWI and accordingly stated in the terms and conditions of employment.*

5.8 SECURITY

5.8.1 Personal data will be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification, or destruction. This applies regardless of whether data is processed electronically or in paper form.

5.8.2 Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification).

5.8.3 The technical and organizational measures for protecting personal data are part of CRWI's IT-MIS management and must be aligned continuously to the technical developments and organizational changes.

5.9 RETENTION OF DATA

5.9.1 The retention period of any category of Personal Data not specifically defined in this or any other CRWI Policy (CRWI Data Retention Policy) and unless otherwise specified by applicable law, the required retention period for any Personal Data record will be deemed to be seven years from the date of creation of the record.

5.10 DESTRUCTION OF DATA

5.10.1 At the end of the retention period, all documents should be destroyed as follows:

- Physical documents should be destroyed securely (crosscut shredding or licensed secure disposal company).
- Electronic documents should be deleted and removed from recycling bins or discarded as per the CRWI ITAD Guideline
- Automated purge routines will be used to remove records from databases and IT systems (such as SharePoint, OneDrive). This will be managed by IT Unit of CRWI

5.10.2 In some circumstances (such as legal action or police investigation), CRWI will be required to provide all relevant documentation. This means these documents must not be destroyed until the legal action/investigation has completed. If any staff receives a request for information in these kinds of circumstances, they must inform the Data Protection office at the earliest.

5.10.3 The DPO will promptly inform all staff of any suspension in the further disposal of documents.

5.11 DATA PROTECTION CONTROL

5.11.1 Compliance with the CRWI Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other control measures.

5.11.2 The performance of these controls is the responsibility of CRWI's Executive Director or appointed representative by the Executive Director

5.11.3 The results of the data protection controls performed by the appointed representative must be reported to the Executive Director. The CRWI Board must be informed of the primary results as part of the related reporting duties.

5.11.4 The results of data protection controls will be made available to the responsible data protection authority only on request. The responsible data protection authority can perform its own controls of compliance with the regulations of this Data Protection Policy, as permitted under national law.

6 CHAPTER SIX: VIOLATION- GRIEVANCE REDRESSAL, REPORTING AND MANAGEMENT

6.1 VIOLATION AND GRIEVANCE REDRESSAL

6.1.1 Failure to comply with the Data Protection Policy or to deliberately violate the rules set in the policy will result in the launch of an appropriate investigation by CRWI.

6.1.2 Depending on the gravity of the suspicion or accusations, CRWI may suspend staff or relations with other stakeholders during the investigation. This will not be subject to challenge.

6.1.3 Depending on the outcome of the independent investigation, if it comes to light that anyone associated with CRWI has deliberately violated the rules set in the policy for its personal profit or any other usage of personal data or has systematically and deliberately contravened with the principles and standards contained in this document, CRWI will take immediate disciplinary action and any other action which may be appropriate to the circumstances. This may mean, for example, for:

- Staff - disciplinary action/dismissal
- Trustees, officers and interns - ending the relationship with the organization.
- Partners - withdrawal of support/termination of partnership.
- Contractors and consultants - termination of contract

6.1.4 Depending on the nature, circumstances and location of the case and violation, CRWI will also consider involving authorities such as the police to ensure the protection of personal data and possible or actual victims.

6.1.5 If any staff member has any grievance against any other staff of the same location or from any other location, pertaining to breach of protection of personal data, the staff can take assistance of CRWI grievance addressal mechanism.

6.2 TYPES OF BREACH

6.2.1 An event or action which may compromise the confidentiality, integrity or availability of systems or data (either accidentally or deliberately) and cause damage to CRWI's information assets and/or reputation.

6.2.2 An incident includes but is not limited to the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper records).
- Equipment theft or failure.
- Unauthorized use of access to or modification of data or information systems.
- Unauthorized disclosure of sensitive / confidential data.
- Hacking or phishing attack.
- Human error.
- Information obtained by deception.
- Deliberate destruction of assets containing data.

6.3 REPORTING

6.3.1 The reporting of suspected or actual violations of this policy is a professional and legal obligation of all staff and entities or individuals working on behalf of CRWI. Failure to report violations will lead to suitable action as deemed necessary by the CRWI to protect its interests.

6.3.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as possible.

6.3.3 As much information as possible should be included when reporting, including:

- When the breach occurred (dates and times).

- Where the breach occurred (location/ venue/ office)
- How the breach occurred (process or incidence)
- Name, location, and job title of the person reporting the breach.
- The nature of the information which has been compromised (sensitivity of the data)
- Who was involved?
- Any other relevant information.

6.3.4 CRWI encourages its staff and stakeholders to report suspected cases which involve any CRWI staff, consultants, board members, guests, or staff of CRWI's partner organizations, their board members, staff and or suppliers. Relevant policies such as the Whistle Blower Policy etc. will come into force to protect the identity of the complainant.

6.3.5 CRWI will not tolerate false accusations which are designed to intentionally damage a staff's reputation. Anyone found making false accusations will be subject to investigation and disciplinary action under other policies of the organization.

6.4 MANAGEMENT

6.4.1 The Data Protection Officer will determine if the breach is still occurring or already occurred. If occurring, appropriate steps will be taken immediately to contain the breach.

6.4.2 The Data Protection Officer under the guidance of the Executive Director will form a team comprising staff from relevant units and locations. The team size will be of a minimum of three people.

6.4.3 An initial assessment will be made by the Data Protection Officer in liaison with relevant staff to establish the severity of the breach and wo will take the lead investigating the breach.

6.4.4 Investigation will be undertaken by the Data Protection Officer or an appointed member of staff immediately and wherever possible within 24 hours of the breach being discovered / reported.

6.4.5 The Data Protection Officer and relevant staff will assess the risks associated with the breach, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6.4.6 The Data Protection Officer will determine who needs to be notified of the breach by considering whether there are any legal/contractual notification requirements; or whether notification would assist the individual affected – could they act on the information to mitigate risks or whether notification would help prevent the unauthorized or unlawful use of personal data or would notification help CRWI meet its obligations under the data protection principle.

6.4.7 The DPO will report the breach, to the Executive Director within four hours from the time breach was reported or identified and may also in some cases be required to inform others about the breach such as: the police and or any individual directly affected by the breach.

6.4.8 The Data Protection Officer must consider notifying third parties such as the insurers, bank or credit card companies, the Societies Registrar. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

6.4.9 The Data Protection Officer will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

6.4.10 Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the data involved.

6.4.11 Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks.

6.4.12 Individuals will also be provided with a way in which they can contact CRWI for further information or to ask questions about what has occurred.

6.4.13 All actions will be recorded by the Data Protection Officer.

6.4.14 Annually the Data Protection Officer will gather the relevant people and run through a test scenario to ensure the Incident management procedure is functional. Results of this will be recorded and stored.

6.4.15 Once the initial incident is contained, the Data Protection Officer will carry out a full review of the causes of the breach, the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

6.4.16 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimize the risk of similar incidents occurring.

7 CHAPTER SEVEN: DATA PROTECTION OFFICER

7.1 APPOINTMENT

7.1.1 A Data Protection Officer shall be appointed by the Executive Director of CRWI and report directly to him/her/ them.

7.1.2 The Data Protection Officer shall act independently, in a neutral and impartial manner.

7.2 DUTIES

7.2.1 The Data Protection Officer shall monitor the application of this Policy.

7.2.2 The Data Protection Officer shall, on request or on his/her initiative, advise individuals on their rights and Data Controllers on their rights and obligations.

7.3 COOPERATION OF DATA CONTROLLERS WITH THE DATA PROTECTION OFFICER

7.3.1 Data Controllers shall cooperate with the Data Protection Officer by assisting the Data Protection Officer and making available any information necessary for the Data Protection Officer to carry out his/her tasks.

7.3.2 Data Controllers shall involve the Data Protection Officer in the process of designing new information systems and ensure that measures of data protection are built in those systems from the beginning.

8 CHAPTER EIGHT: ACKNOWLEDGEMENT AND SETTLEMENT OF CLAIMS

8.1 PROCESS AND TIMEFRAME

8.1.1 Any individual may complain in writing to the Data Protection Officer (dpo@CRWI.org) about any matter relating to his/her Personal Data, including any Personal Data Breach.

8.1.2 The Data Protection Officer must acknowledge receipt in writing and decide on the complaint within ten working days. The Data Protection Officer may extend the time limit to another twenty (20) days if it considers the complaint requires further assessment. In such a case, the Data Protection Officer shall give notice of the extension to the complainant in writing.

8.1.3 Any individual may further challenge the decision of the Data Protection Officer if he/she/ they consider it affects him/her/ them adversely in accordance with the procedures established below.

8.1.4 Any Staff may challenge the decision of the Data Protection Officer if he/she/ they consider it affects him/her/ them adversely. He/she shall proceed in accordance with the dispute settlement procedures as detailed in the applicable CRWI Policy.

8.1.5 Any other individual challenging a decision of the Data Protection Officer which he/she/ they consider affecting him/her/ them adversely, shall only and exclusively follow the procedure laid down in other policies of the organization.

9 IMPLEMENTATION OF DATA PROTECTION POLICY

This data protection policy is a comprehensive policy that builds trust and protection of the rights of the individuals and accountability of CRWI towards safeguarding these. This will be implemented in the same manner as part of the overall policies of CRWI and governance of the organization and treated in the same manner.

9.1 PART OF THE COMPREHENSIVE POLICY AND GUIDELINES HANDBOOK

9.1.1 This policy becomes part of the comprehensive handbook of Policies and Guidelines in force at CRWI. It will be appropriately introduced to staff so that all staff at all levels understand the importance and their adherence to it.

9.2 SUMMARIZED VERSION

9.2.1 If required, a summarized version of the Data Protection Policy will be prepared that covers the main aspects of the policy and assists in drawing up a general understanding about the policy and expectations from the staff regarding data protection.

9.3 TRAINING AND SUPERVISION

9.3.1 Staff shall undertake data protection training within 3 months of joining CRWI.

9.3.2 All CRWI staff at all levels are required to undergo CRWI's mandatory Data Protection Training Module every year.

9.3.3 Training to be provided according to individual roles and work.

9.3.4 The designated person by the Executive Director of CRWI will supervise and conduct the training program for all staff and refresher at intervals of at least six months.

9.4 INFORMATION TO EXTERNAL ENTITY

9.4.1 Wherever an external entity is engaged either in data processing or realization of actual work such as vendors, consultants, contractors, partners, etc. will be provided a copy of the policy in paper or digital form to comply with it.

9.5 INSERTION AS CLAUSE

9.5.1 All contracts and agreements with external entities to have the clause of compliance with "CRWI Data Protection Policy."

10 CHAPTER TEN - COVERAGE UNDER OTHER POLICIES

Other policies and guidelines will come into force as supplements to safeguard the rights of staff and individuals while dealing subjects under Data Protection Policy.