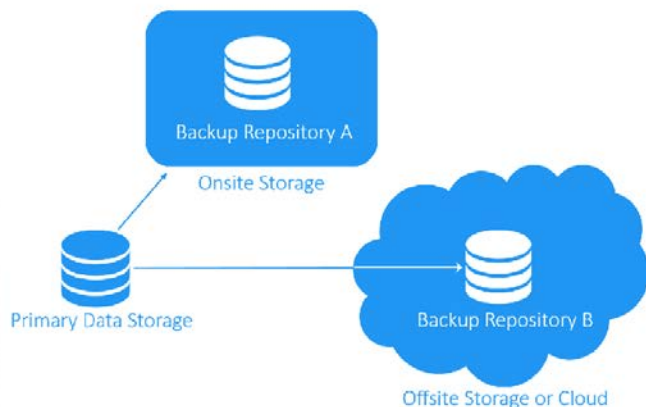




# POLICY ON DATA PROTECTION AND PRIVACY

(PROTECTION, TRANSPARENCY, AND ACCOUNTABILITY)

Sabuj Sangha's Code of Ethics & Business Conduct at Work



**SABUJ SANGHA**

**30/9, Rajdanga Main Road, (East) Kolkata, West Bengal- 700 107**



## I. PREFACE

The Organisation has adopted the Code of Ethics & Business Conduct, which lays down the principles and standards that should govern the actions of the Organisation and its employees.

The right to privacy is a fundamental right and it is necessary to protect personal as well as organizational data as an essential facet of informational privacy. The data as a critical means of communication between persons and thereby it is necessary to create a collective culture that fosters a free and fair digital world, respecting the informational privacy of individuals and organization.

Sabuj Sangha needs to gather and use certain information about individuals. These can include beneficiaries, suppliers, business contacts, employees, and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled, and stored to meet the organization's data protection standards- and to comply with the law.

It is important to make provisions:

- to protect individuals personal data and its usage,
- to create a relationship of trust between persons and organization processing their data,
- to create a framework for implementing organisational and technical measures in processing personal data, and
- to establish a **Data Protection & Privacy Officer** for overseeing data processing.

The Board of Sabuj Sangha keeping the Personal Data Protection Bill, 2018, Govt. of India and Sabuj Sangha's Code of Ethics & Business Conduct into larger consideration, has approved the Policy on Data Protection and Privacy of Sabuj Sangha.

Any actual or potential violation of the Code as such would be a matter of serious concern for the Organisation. The role of employees in pointing out such violations of the Code cannot be undermined. Accordingly, this Policy on Data Protection and Privacy ("the Policy") has been formulated to reinforce the organization's commitment to its values, attitudes, and ethics towards data protection and maintaining the utmost lawful privacy of an individual as well as that of organization.

## II. POLICY

This data protection and privacy policy ensure Sabuj Sangha:

- Complies with data protection law and follow good practice
- Protects the rights of staff, beneficiaries, and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

This policy applies to all staff of Sabuj Sangha and those of Partner organizations, as well as Vendors and Vendor organizations who are in a relationship with Sabuj Sangha. The purpose of this policy is to maintain the privacy of employees, contractors, vendors, interns, associates, and partner organizations, protect their personal information, and ensure compliance with laws and regulations applicable.



The policy covers the responsibility to report all wrongful acts committed to the **Data Protection & Privacy Officer (DPPO)**, who is officially appointed to receive complaints and initiate the investigation. The DPPO will also keep track of all reported cases and report the same to Board.

The Organisation is committed to adhering to the highest standards of ethical, moral, and legal conduct of business operations.

### III. SCOPE

This policy applies to all employees (full-time, part-time, trainees, and those on contractual assignments) of the organization including all associated vendors and partner organizations.

This policy applies to all Sabuj Sangha employees, contractors, vendors, interns, associates, and partners who may receive personal information, have access to personal information collected or processed, or who provide information to the organization, regardless of geographic location. All employees of Sabuj Sangha are expected to support the privacy policy and principles when they collect and/or handle personal information, or are involved in the process of maintaining or disposing of personal information. This policy provides the information meeting successfully the organization's commitment to data privacy.

All partner organizations and any Third-Party working with or for Sabuj Sangha, who have or may have access to personal information, will be expected to have read, understood, and complied with this policy. No Third Party may access personal information held by the organization without having first entered into a confidentiality agreement.

### IV. DATA PROTECTION RISKS/APPLICABILITY

This Policy covers all directors, managers, employees, third-party vendors, consultants, interns, and partners operating out of any location of the Organisation. This policy helps to protect Sabuj Sangha from some very real data security risks, including:

- **Breaches of confidentiality:** For instance, information being given out inappropriately;
- **Failing to offer a choice:** For instance, all individuals should be free to choose how the organization uses data relating to them;
- **Reputational damage:** For instance, the organization could suffer if hackers successfully gained access to sensitive data;
- **Data theft:** For instance, the organization could suffer if any data related to Sabuj Sangha's programs, financials, contracts, survey data, beneficiaries details, funders documents, plans, etc.

### V. RESPONSIBILITIES

Everyone who works for or with Sabuj Sangha has some responsibility for ensuring data is collected, stored, and handled appropriately.



Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Director, Sabuj Sangha is ultimately responsible for ensuring that organization meets its legal obligations.
- The **DPPO** is responsible for:
  - Keeping the Director updated about data protection responsibilities, risks, and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data Sabuj Sangha holds about them (also called ‘subject access requests’).
  - Checking and approving any contracts or agreements with third parties that may handle the organization’s sensitive data.
- The **IT manager or assigned person** is responsible for:
  - Ensuring all systems, services, and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software are functioning properly.
  - Evaluating any third-party services the organization is considering using to store or process data. For instance, cloud computing services, etc.
- The **marketing manager or assigned person** is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Custodian for the Data Protection & Privacy Policy shall be the DPPO. The DPPO shall be responsible for the maintenance and accuracy of this policy. Any queries regarding the implementation of this Policy shall be directed to the DPPO.

This policy shall be reviewed for updates by the Data Protection & Privacy Review Team in consultations with the DPPO, the Director, and other concerned stakeholders on an annual basis. Additionally, the data privacy policy shall be updated in-line with any major changes within the organization’s operating environment or on recommendations provided by internal/ external auditors.

## **VI. GENERAL STAFF GUIDELINES**

- The only people able to access data covered by this policy should be those who need it for their work.



- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Sabuj Sangha will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the organization or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the DPPO if they are unsure about any aspect of data protection.

## **VII. DATA STORAGE**

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller or the person assigned.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services or as decided by Sabuj Sangha from time to time.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the organization's standard backup procedures.



- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall.

### **VIII. DATA USE**

Personal data is of no value to Sabuj Sangha unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside the specified region.
- Employees should not save copies of personal data on their computers. Always access and update the central copy of any data.

### **IX. DATA ACCURACY**

The law requires Sabuj Sangha to take reasonable steps to ensure data is kept accurate and up-to-date. The more important it is that the personal data is accurate, the greater the effort Sabuj Sangha should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- Sabuj Sangha will make it easy for data subjects to update the information the organization holds about them.
- Data should be updated as inaccuracies are discovered.

### **X. SUBJECT ACCESS REQUESTS**

All individuals who are the subject of personal data held by Sabuj Sangha are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed on how to keep it up to date.
- Be informed about how the organization is meeting its data protection obligations.

If an individual contacts the organization requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email,



addressed to the data controller at the designated person's email id. The data controller can supply a standard request form, although individuals do not have to use this. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

#### **XI. DISCLOSING DATA FOR OTHER REASONS**

In certain circumstances, personal data has to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Sabuj Sangha will disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the organization's legal advisers where necessary.

#### **XII. PROVIDING INFORMATION**

Sabuj Sangha aims to ensure that individuals are aware that their data is being processed and that they understand:

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

To these ends, the organization has a privacy statement, setting out how data relating to individuals is used by the organization.

#### **XIII. POLICY COMPLIANCE**

**“Data Protection & Privacy Review Team (DPPRT)”** as formed by the organization to ensure continuous compliance monitoring through the implementation of compliance measurements and periodic review processes shall review compliance to the data protection & privacy policy on an annual basis. It will also take care of the detection of data breaches proactively.

In cases where non-compliance is identified, the DPPO shall review the reasons for such non-compliance along with a plan for remediation and report them to DPPRT.

Depending on the conclusions of the review, the need for a revision to the policy may be identified. In instances of persistent non-compliance by the individuals concerned, they shall be subject to action following the Sabuj Sangha's Disciplinary Policy.

#### **XIV. DATA PROTECTION & PRIVACY PRINCIPLES**

This Policy describes **generally accepted privacy principles (GAPP)** for the protection and appropriate use of personal information at Sabuj Sangha. These principles shall govern the use, collection, disposal and transfer of personal information, except as specifically provided by this Policy or as required by applicable laws:

- **Notice:** Sabuj Sangha shall provide data subjects with a notice about how it collects, uses, retains, and discloses personal information about them.
- **Choice and Consent:** Sabuj Sangha shall give data subjects the choices and obtain their consent regarding how it collects, uses, and discloses their personal information.



- **Rights of Data subject:** Sabuj Sangha shall provide individuals with the right to control their personal information, which includes the right to access, modify, erase, restrict, transmit, or object to certain uses of their information and for withdrawal of earlier given consent to the notice.
- **Collection:** Sabuj Sangha shall collect personal information from data subjects only for the purposes identified in the privacy notice/contract agreements and only to provide the requested product or service.
- **Use, Retention, and Disposal:** Sabuj Sangha shall only use personal information that has been collected for the purposes identified in the privacy notice/contract agreements and by the consent that the data subject shall provide. Sabuj Sangha shall not retain personal information longer than is necessary to fulfill the purposes for which it was collected and to maintain reasonable business records. Sabuj Sangha shall dispose of the personal information once it has served its intended purpose or as specified by the data subject.
- **Access:** Sabuj Sangha shall allow data subjects to make inquiries regarding the personal information about them, that Sabuj Sangha shall hold and, when appropriate, shall provide access to their personal information for review, and/or update.
- **Disclosure to Third Parties:** Sabuj Sangha shall disclose personal information to Third Parties/partner organizations only for purposes identified in the privacy notice/contract agreements. Sabuj Sangha shall securely disclose personal information, with assurances of protection by those parties, according to the contracts, laws, and other segments, and, where needed, with the consent of the data subject.
- **Obligations for Sub-processor:** Where a processor (vendor or a third party acting on behalf of Sabuj Sangha's data processor) engages another processor (Sub-processor) for carrying out specific processing activities on behalf of Sabuj Sangha (controller), the same data protection obligations as set out in the contract or other legal act between Sabuj Sangha and the processor shall be applicable on the Sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of **General Data Protection Regulation (GDPR)**. Where the Sub-processor fails to fulfill its data protection obligations, the initial processor (relevant vendor or a third party acting on behalf of Sabuj Sangha's data processor) shall remain fully liable to Sabuj Sangha for the performance of that Sub-processor's obligations.
- **Security for Privacy:** Sabuj Sangha shall protect personal information from unauthorized access, data leakage, and misuse.
- **Quality:** Sabuj Sangha shall take steps to ensure that personal information in its records is accurate and relevant to the purposes for which it was collected.
- **Monitoring and Enforcement:** Sabuj Sangha shall monitor compliance with its privacy policies, both internally and with Third Parties, and establish the processes to address inquiries, complaints, and disputes.





## **XV. NOTICE**

Notice shall be made readily accessible and available to data subjects before or at the time of collection of personal information or otherwise, notice shall be provided as soon as practical thereafter. Notice shall be displayed clearly and conspicuously and shall be provided online (e.g. by posting it on the home portal, website, sending emails, newsletters, etc.) and/or offline methods (e.g. through posts, couriers, etc.). All the websites and any program or service that collects personal information internally, shall have a privacy notice.

In case of any external transfer of personal information, a notice sufficiently before the transfer shall inform the data subjects.

Privacy notices may include:

- the organization's operating jurisdictions, third parties involved, partner organizations and affiliates, lines of business/works, locations;
- types of personal information collected, sources of information who is collecting the personal information, including contact information;
- the purpose of collecting personal information;
- assurance that the personal information will be used only for the purpose identified in the notice and only if the implicit and/or explicit consent is provided unless a law or regulation specifically requires otherwise;
- any choices the data subject have regarding the use or disclosure of the information, the process, and the data subject shall follow to exercise the choices;
- the process for a data subject to change contact preferences and ways in which the consent is obtained;
- collection process and how the information is collected; how the information is used including any onward transfer to Third-Parties;
- retention and disposal process for personal information, assurance that the personal information to be retained only as long as necessary to fulfill the stated purposes, or for a period specifically required by law or regulation and will be disposed-off securely or made anonymous post the identified purpose is completed;
- process of accessing personal information, the costs associated for accessing personal information (if any), process to update/correct the personal information, the resolution of disagreements related to personal information, how the information is protected from unauthorized access or use;
- how users will be notified of any changes made to privacy notice;
- disclosure process for Third Parties, the assurance that the personal information is disclosed to Third Parties only for the purpose identified, the remedial actions in place for any misuse of personal information by the Third Parties;
- security measures in place to protect the personal information, ways of maintaining the quality of personal information;



- monitoring and enforcement mechanisms in place, description of the complaint channels available to data subjects; how the internal personnel, key stakeholders and the beneficiaries/organizations/vendors can contact Sabuj Sangha related to any privacy complaints or breaches, relevant contact information and/or other reporting methods through which the complaints and/or breaches could be registered;
- Consequences of not providing the requested information.

## **XVI. CHOICE & CONSENT**

Choice refers to the options the data subjects are offered regarding the collection and use of their personal information. Consent refers to their agreement to the collection and uses, often expressed by how they exercise a choice option.

- Sabuj Sangha shall establish systems for the collection and documentation of data subject consents to the collection, processing, and/or transfer of personal data.
- Data subjects shall be informed about the choices available to them for the collection, use, and disclosure of personal information.
- The consent shall be obtained (in writing or electronically) from the data subjects before or at the time of collecting personal information or as soon as practical thereafter.
- The changes to a data subject's preferences shall be managed and documented. Consent or withdrawal of consent shall be documented appropriately.
- The choices shall be implemented in a timely fashion and respected. If personal information is to be used for purposes not identified in the notice/contract agreements at the time of collection, the new purpose shall be documented, the data subject shall be notified, and consent shall be obtained before such new use or purpose.
- The data subject shall be notified if the data collected is used for marketing purposes, advertisements, etc.
- Sabuj Sangha shall review the privacy policies of the Third Parties and types of the consent of Third Parties before accepting personal information from Third-Party data sources.

## **XVII. COLLECTION OF PERSONAL INFORMATION**

Personal information may be collected online or offline. Regardless of the collection method, the same privacy protection shall apply to all personal information.

- Personal information shall not be collected unless either of the following is fulfilled:
  - the data subject has provided a valid, informed and free consent;
  - processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract;
  - processing is necessary for compliance with the organizations legal obligation;
  - processing is necessary to protect the vital interests of the data subject; or
  - processing is necessary for the performance of a task carried out in the public interest



- Data subjects shall not be required to provide more personal information than is necessary for the provision of the product or service that the data subject has requested or authorized. If any data not needed for providing a service or product is requested, such fields shall be clearly labeled as optional. The collection of personal information shall be avoided or limited when reasonably possible.
- Personal information shall be de-identified when the purposes of data collection can be achieved without personally identifiable information, at a reasonable cost.
- When using vendors to collect personal information on the behalf of Sabuj Sangha, it shall ensure that the vendors comply with the privacy requirements of Sabuj Sangha as defined in this Policy.
- Sabuj Sangha shall at minimum, annually review and monitor the information collected, the consent obtained and the notice/contract agreement identifying the purpose.
- The project team/support function shall obtain approval from the IT Security team before adopting the new methods for collecting personal information electronically.
- Sabuj Sangha shall review the privacy policies and collection methods of Third-Parties before accepting personal information from Third-Party data sources.

#### **XVIII. USE, RETENTION, AND DISPOSAL**

- Personal information may only be used for the purposes identified in the notice/contract agreements and only if the data subject has given consent;
- Personal information shall be retained for as long as necessary for business purposes identified in the notice/contract agreements at the time of collection or subsequently authorized by the data subjects.
- When the use of personal information is no longer necessary for business purposes, a method shall be in place to ensure that the information is destroyed in a manner sufficient to prevent unauthorized access to that information or is de-identified in a manner sufficient to make the data non-personally identifiable.
- Sabuj Sangha shall have a documented process to communicate changes in retention periods of personal information required by the business to the data subjects who are authorized to request those changes.
- Personal information shall be erased if their storage violates any of the data protection rules or if knowledge of the data is no longer required by Sabuj Sangha or for the benefit of the data subject. Additionally, Sabuj Sangha has the right to retain the personnel information for legal and regulatory purposes and as per applicable data privacy laws.
- Sabuj Sangha shall perform an internal audit on an annual basis to ensure that personal information collected is used, retained, and disposed-off in compliance with the organization's data privacy policy.

#### **XIX. ACCESS**

Sabuj Sangha shall establish a mechanism to enable and facilitate the exercise of data subject's rights of access, blockage, erasure, opposition, rectification, and, where



appropriate or required by applicable law, a system for giving notice of inappropriate exposure of personal information.

- Data subjects shall be entitled to obtain the details about their personal information upon a request made and outlined in writing. Sabuj Sangha shall provide its response to a request within 72 hours of receipt of a written request.
- The data subjects shall have the right to require Sabuj Sangha to correct or supplement erroneous, misleading, outdated, or incomplete personal information.
- Requests for access to or rectification of personal information shall be directed, at the data subject's option, to the manager of the project team or support function responsible for the personal information.
- The privacy coordinators shall record and document each access request as it is received and the corresponding action taken.
- Sabuj Sangha shall provide personal information to the data subjects in a plain simple format, which is understandable (not in any code format).

## **XX. DISCLOSURE TO THIRD PARTIES**

Data Subject shall be informed in the privacy notice/contract agreement if personal information shall be disclosed to Third Parties/partner firms, and it shall be disclosed only for the purposes described in the privacy notice/contract agreements and for which the data subject has provided consent.

- Personal information of data subjects may be disclosed to the Third Parties/partner organizations only for reasons consistent with the purposes identified in the notice/contract agreements or other purposes authorized by law.
- Sabuj Sangha shall notify the data subjects before disclosing personal information to Third Parties/partner organizations for purposes not previously identified in the notice/contract agreements.
- Sabuj Sangha shall communicate the privacy practices, procedures, and requirements for data privacy and protection to the Third Parties/partner organizations.
- The Third Parties shall sign a **Non-Disclosure Agreement (NDA)** with Sabuj Sangha before any personal information is disclosed to the Third Parties partner organizations. The NDA shall include the terms on non-disclosure of information.

## **XXI. SECURITY**

Information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred, and disposed of by Sabuj Sangha.

- Information asset labeling and handling guidelines shall include controls specific to the storage, retention, and transfer of personal information.
- Management shall establish procedures that maintain the logical and physical security of personal information.



- Management shall establish procedures that ensure the protection of personal information against accidental disclosure due to natural disasters and environmental hazards. Incident response protocols are established and maintained to deal with incidents concerning personal data or privacy practices.
- Individuals noticing or becoming aware of any breach of personal data shall notify the DPPO (by emailing at [data.privacy@sabujsangha.org](mailto:data.privacy@sabujsangha.org)) within 24 hours. It shall be the DPPO's responsibility to analyze and act on the intimation of the same within 48 hours; furthermore under the Sabuj Sangha Data Protection and Privacy Policy (wherever applicable).

## **XXII. QUALITY**

Sabuj Sangha shall maintain data integrity and quality, as appropriate for the intended purpose of personal data collection and use and ensure data is reliable, accurate, complete, and current.

- For this purpose, the DPPO and other privacy coordinators shall have systems and procedures in place to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.
- Sabuj Sangha shall perform an annual assessment on the personal information collected to check for accuracy, completeness, and relevance of the personal information.

## **XXIII. MONITORING AND ENFORCEMENT**

### **(i). DISPUTE RESOLUTION AND RECOURSE**

Sabuj Sangha shall define and document a Data Protection and Privacy policy, which addresses the privacy-related incidents and breaches.

- The incident and breach management program includes a clear escalation path up to the executive management, legal counsel, and the board based on the type and/or severity of the privacy incident/breach. It shall define a process to register all the incidents/complaints and queries related to data privacy
- Sabuj Sangha shall perform a periodic review of all the complaints related to data privacy to ensure that all the complaints are resolved promptly and resolutions are documented and communicated to the data subjects as the case may be.
- An escalation process for unresolved complaints and disputes, which shall be designed and documented.
- Communication of privacy incident/breach reporting channels and the escalation matrix shall be provided to all the data subjects as the case may be.

### **(ii). DISPUTE RESOLUTION AND ESCALATION PROCESS FOR EMPLOYEES**

Employees with inquiries or complaints about the processing of their personal information shall first discuss the matter with their immediate supervisor. If the employee does not wish to raise an inquiry or complaint with an immediate manager, or if the manager and employee are unable to reach a satisfactory resolution of the issues raised, the employee



shall email at [data.privacy@sabujsangha.org](mailto:data.privacy@sabujsangha.org) to bring the issue to the attention of the DPPO.

**(iii). DISPUTE RESOLUTION AND ESCALATION PROCESS FOR THIRD PARTY**

Beneficiaries/Third Party with inquiries or complaints about the processing of their personal information shall bring the matter to the attention of the DPPO in writing. Any disputes concerning the processing of the personal information of non-employees shall be resolved through arbitration.

**(iv). COMPLIANCE REVIEW**

The DPPRT shall conduct an internal audit annually (at minimum) to ensure compliance with the established privacy policies and applicable laws.

- The internal audit shall consist of a review of the following:
  - personal information collected from data subjects;
  - the purposes of the data collection and processing;
  - the actual uses of the data;
  - disclosures made about the purposes of the collection and use of such data;
  - the existence and scope of any data subject consents to such activities;
  - any legal obligations regarding the collection and processing of such data, and
  - the scope, sufficiency, and implementation status of security measures.
- The DPPRT shall document all the instances of non-compliance with privacy policies and procedures and report the same with the **Privacy Management Committee** headed by the Director, Sabuj Sangha.
- The DPPO along with Privacy Coordinators shall take action on the findings from the internal audit and work on the recommendations for improvement of the privacy posture.
- Any changes made to the policies shall be communicated to all the employees, the stakeholders, and the beneficiaries/funders (wherever required).

**XXIV. DEFINITIONS**

- **“Data Subject”** means a data subject who is the subject of personal data.
- **“Personal Data or Personally Identifiable Information (PII)”** means any information about an individual (the data subject) which can be used to distinguish or trace an individual’s identity or, any other information that is linked or linkable to an individual (Examples included but not limited to: Name, Address, Date of birth, etc.)
- **“Sensitive Personal Information (SPI)”** means personal data consisting of information but not limited to the following attributes of the data subject:
  - password;
  - financial information such as bank account or credit card or debit card or other payment instrument details ;
  - physical, physiological and mental health condition;



- sexual orientation;
- medical records and history;
- genetic or biometric information;
- racial and ethical origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- any detail relating to the above clauses as provided to the organization; and
- any of the information received under above clauses by the partner organizations or stakeholders for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for these rules.

- **“Third Party”** means all external parties – contractors, interns, summer trainees, and vendors – who have access to Sabuj Sangha information assets or information systems.
- **“Disciplinary Action”** means any action that can be taken on the completion of /during the investigation proceedings including but not limited to a warning, imposition of fine, suspension from official duties, or any such action as is deemed to be fit considering the gravity of the matter.
- **“Data Protection and Security”** means anyone collecting personal and beneficiaries information must fairly and lawfully process it, process it only for limited, specifically stated purposes, use the information in a way that is adequate, relevant and not excessive, use the information accurately, keep the information on file no longer than necessary, process the information following your legal rights, keep the information secure and never transfer the information to others unlawfully and outside the country without adequate protection;
- **“Employee”** means every employee of Organisation (whether working in India or abroad)
- **“Complaint”** means the reporting of any such breach of privacy or data protection violation to the DPPRT made in good faith would constitute a complaint.
- **“Data Protection & Privacy Review Team (DPPRT)”** means a team as formed by the organization to ensure continuous compliance monitoring through the implementation of compliance measurements and periodic review processes
- **“Privacy Management Committee”** means the Committee constituted by the Board of the Organisation by the applicable law headed by the Director, Sabuj Sangha.
- **“Data Protection & Privacy Officer (DPPO)”** means an officer who is officially appointed to receive complaints and initiate the investigation.

## XXV. MONITORING AND EVALUATION

Sabuj Sangha recognises the importance of monitoring this data protection and privacy policy and will ensure that it anonymously collects statistics and data as to how it is used and whether or not it is effective.



Supervisors, managers and those responsible for dealing with any privacy breaches will report on compliance with this policy, including the number of incidents, how they were dealt with, and any recommendations made. This will be done yearly. As a result of this report, the organization will evaluate the effectiveness of this policy and make any changes needed.

#### **XXVI. NOTIFICATION**

1. All Managers are required to notify and communicate the existence and contents of this policy to the employees of their department and all new employees respectively.
2. The onus of making the Partners aware of their responsibilities vests with Director or the person assigned for the purpose by Sabuj Sangha Management who will ensure that program staff make Partners aware of their responsibility and make them understand that they may report any wrongful conduct of Sabuj Sangha staff in the execution of a Partnership agreement.

#### **XXVII. RETENTION OF DOCUMENTS**

All Protected Disclosures in writing or documented along with the results of the investigation relating thereto, shall be retained by Sabuj Sangha for a minimum period of 7 years as a normal practice.

#### **XXVIII. COMMUNICATION**

1. This policy as amended from time to time shall be disclosed on the website of the Organization and in the report of the Board of the Organization.
2. The Audit Committee reviews the policy and its implementation periodically and is provided a quarterly update on the status of various complaints received and investigated.

#### **XXIX. CONCLUSION:**

In conclusion, the organization reiterates its commitment to providing its employees, a workplace having its data and privacy protected. The onus is on the employees and all concerned stakeholders to protect the data and maintain its privacy as well.