NNSWA
IT Policy
2023

NNSWA

Nepal National Social Welfare Association

Kanchanpur

NNSWA IT/Data Protection Policy-2023

NNSWA Information Technology Guideline Approved by General Assembly on August 18th 2023

NNSWA
Nepal National Social Welfare Association

Nepal National Social Welfare Association (NNSWA)
Airport Road, Bheemdatt (Mahendranagar) Municipality, Ward-# 18,
District-Kanchanpur
Province # 7, Nepal
Phone: 00-977-99-522182
Email: info@nnswa.org.np
Website: www.nnswa.org.np

विषय सूची

विषय:

दुई शब्द:

Section 'A'

Organizational Introduction

Section 'B'

Information Technology/Data Protection Policy 2023

a. Ownership:
b. Retention:
c. Accountability:
d. Security:
e. Ethical behavior and responsible Use:

1.3 Software:
a. Ownership:
b. Supported software:
c. Prohibited software:
d. Shareware:
e. Purchase of software:
f. Accountability:
g. Ethical behavior and responsible Use:

1.4 Email:
a. Ownership
b. Retention
c. Monitoring
d. Accountability
e. Security
f. Ethical Behavior and Responsible Use
g. Email signature

1.5 Server Back Up/Protection:
a. Staff Responsibilities and Accountability:
b. Backup Criteria:
c. Restore Request procedure:
d. Off Site Backup:
e. Defining what is to be backed up:
f. Types of data backup:
g. Storage medium:

2 Data Protection Procedures:

2.1 SCOPE OF THE PRODUCER:
2.2 GOVERNING LAW
2.3 APPLICABILITY OF THE Policy:
2.4 PERSONAL INFORMATION:
2.5 COLLECTION OF PERSONAL INFORMATION:
2.6 PROCESSING/USE OF PERSONAL INFROMATION:
2.7 RETENTION OF PERSONAL INFORMATION:
2.8 TRANSFER OF DATA:
2.9 RESPONSIBILITY OF THE PUBLIC ENTITY:
2.9.1 RIGHTS OF INDIVIDUALS:
2.9.2 BREACH OF DATA:
2.9.3 IMPLEMENTATION OF THE POLICY:

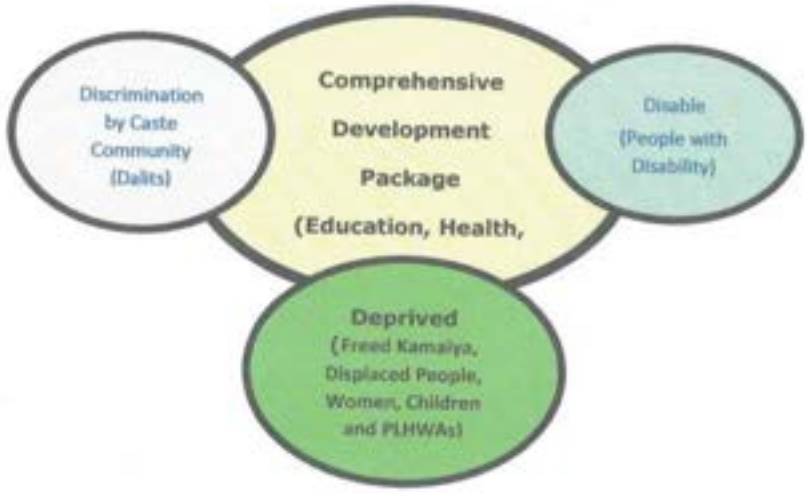
7. Target Groups

- Discriminated Community by Caste (Dalit)
- Disable (People with Disability)
- Deprived (Freed Kamaiya, Displaced People, Women, Children and PLHWAs)

8. Strategies

- Partnership-With the government, donors, INGOs, local NGOs and CBOs
- Participatory Integrated Rural Development
- Gender programming
- Rights based programming and Networking, Alliance and Coalition Building

9. Development Philosophy/Strategy of NNSWA



10. NNSWA Executive Board

The General Members constitute the General Assembly of NNSWA 11 members of this General Assembly constitute an Executive Committee. Executive Members are elected by the General assembly for a term of 5 years. The Executive Committee has 6 Office Bearers (President, Vice-president, General Secretary, Secretary, Treasurer and Vice-treasurer) and 5 Executive Members. The Executive Committee is the legally constituted body responsible for providing strategic and policy direction to NNSWA.

11. Core Management Team

Core Management Team (CMT) is the very power full committee where President and Secretary General from Executive Board and Executive Director from the Employees are the members. This committee has the power to make decisions on any aspect of the situation. The president is the coordinator for this committee. The Secretary General and Executive Director are members. Mostly this committee will be active during an emergency; any problems need to be solved. The committee has power to provide final decision on programmatic and any grievances, any case from the sub committees (e.g., Child Safety, Sexual Harassment, Grievance etc.).

12. Senior Management Team (SMT)

The Senior Management Committee (SMT) provides operational leadership. The Management Committee also serves as a bridge between the Executive Committee and NNSWA's programs. The NNSWA program operational is managed by the SMT under the planned programs. The human resource management for projects and coordination to the employee are the major activities of SMT of NNSWA. Senior topmost staff will be involved in the SMT. Executive director will be the coordinator for the SMT. Executive Director will nominate the members among the programs/projects and representative of executive board. The executive committee of NNSWA will be indorsed the SMT and committee will be effective.

13. Branch Offices:

The district chapter of NNSWA will also apply this policy as central office mended. The district office will allow developing their local policy for fulfills their local requirement, but the local policy should not contradict or supersede the NNSWA central policies.

14. Policy Amendment:

The terms, conditions, rules, and regulations of this policy may be amended at any time if deemed necessary, through written amendments issued by the NNSWA, Executive Director. This may be done as follows:

d) External Requirements:

Due to any reason of national environment is not favorable for the organization or the rules and regulation of Government of Nepal that pushes to amendment the policy and in such cases, the Executive Director will be authority to issue a written amendment to this policy in consultation with Executive Board, SMT and branch office program manager or coordinators.

e) Regular Revised:

Under normal circumstances, any employee may (and are encouraged to) propose changes in the NNSWA Personnel Policy. All proposed changes will normally be considered during periodic review, annual meeting (General Assembly) etc. by the Executive Director. However, critical changes that may be required and made at any time during the process of CMT, SMT and Executive Board meetings.

f) Clarification Rights:

The Executive Director will incorporate all the approved changes in the NNSWA Personnel Policy and disseminate it to all employees. In case of clarification/interpretation, the Executive Director on the behalf of NNSWA Executive Board has the final authority to interpret the policy and to clarify any question or misunderstanding concerning any clauses contained in this policy.

15. Programme Area of NNSWA:

NNSWA's programs are almost entirely grant funded approaches of partnership. NNSWA' program activities are organized into 7 Program Sectors and Themes namely, Education, Health, Livelihood, Economic and Community Development, DRR/HR, Good Governance, Organizational Development, Human Rights and GESI. According to the NNSWA's expertise there will be conducted research and studies as and when required. All sectors will focus their program and activities to the Discriminated Community by Caste (Dalit), Disabled and

Deprived communities as prime target groups. These programs are either directly implemented by NNSWA or in partnership with local organizations.

16. Description of the Program Sectors:

16.1. Education Sector:

To improve the education quality and promoting engagement of parents, improving reading habits of students, creating civic education, involvement of local governments are the focus priorities of the NNSWA. Facilitating and providing expertise of NNSWA for the educational training, new ideology and improving the physical environment of the school are major activities for the NNSWA under education sector. If opportunity is provided to NNSWA by government or any funding agencies, NNSWA will implement Basic Education (BE), early childhood development (ECD) and Non-Formal Education (NFE) as well as physical improvement of the school.

16.2. Health Sector:

NNSWA will implement the following programs and activities under the health sector.

- Nutrition
- Adolescent Reproductive Sexual Health
- Expended Integrated Health Service for HIV and AIDS, PWIDs, CCC
- HIV Test and Counseling (HTC)
- Tuberculosis (TB)
- Trachoma Reduction through School Health Program
- Water and Sanitation (WATSAN)
- Physical Rehabilitation Services with Physiotherapy (Disability)
- Leprosy, Malaria, Safe Motherhood
- Eye, Diabetics etc.

16.3. Livelihood, Economic and Community Development Sector:

- Poverty Alleviation Programme
- Economic Opportunities through Agro-vet program
- Micro Finance (Saving & Credit, Cooperatives, Group loan system)
- Pocket production through value chain and marketing

16.4. DRR/HR Sector:

- LSR, FA and EWS, Mobilizing CDMC, MOCK Drill, Stock Piling
- Humanitarian Response
- Support to Government for Humanitarian Response
- Work for creating resilient community.

16.5. Good Governance Sector:

Under this sector, NNSWA will work for promoting good governance within the organization (NNSWA) and support to promote good governance in local government as well as other civil society. Rights to information (RTI), transparency, accountability, responsibility and the rights of citizens are a major part of the work.

16.6. Organizational Development Sector:

Institutionalization of the system in organization, policy guided activities, skilled staff, system oriented and timely service delivery are a part of the sector. Providing training to the staff, policy

development, HR management and resource mobilization are such activities accumulated within the sector.

16.7. Human Rights and GESI:

Human rights and GESI (Gender Equity and Social Inclusion) will be applying as cross cutting approaches in all programmes, activities, and organizational development part of the NNSWA. The planning of the project or program also applying the HR/GESI throughout the project/program management cycles.

Section 'B'
Information Technology/Data Protection Policy 2023

Nepal National Social Welfare Association (NNSWA) is a civil society organization has been implementing various integrated community development projects in targeted communities based on organizational vision, mission, goal, and objectives from the 1990 AD. Today NNSWA has been accepted by the community and other stakeholders as a development partner. A diversify support partner agency has been believing of NNSWA's integrity, honesty, and transparency for the partnership with NNSWA to implement the project in targeted communities.

Therefore, NNSWA has prepared this Information Technology 2023 to make organizational reorganization among all stakeholders through it's' logo, color and other fundamental items that should be used in NNSWA's working or publicly spread material as visibility.

The following points are obligated to all in NNSWA to their work as NNSWA Information Technology.

2. Information Technology:

1.6 Information Security:

All NNSWA personnel must respect the legitimate interests of the NNSWA. Ethical and acceptable use of information and associated systems and networks must be respected and strictly maintained by all users according to (where appropriate) the principles set out in the NNSWA IT Policy. NNSWA encourages the use of its technical resources; however, they remain the organizational property; are provided to conduct official duties, and are offered on a privileged basis only.

All NNSWA personnel accessing NNSWA's information and communications systems shall:

a. Ensure that they use it for the intended business purpose only.
b. Protect the confidentiality, integrity and availability of those assets.
c. ensure the correct and secure operation of systems supporting the daily operations of NNSWA.
d. Not using the systems in a manner that damages NNSWA's reputation or brand.

All NNSWA personnel involved with system development must embed security as an integral component of the lifecycle (procurement, design, development, commissioning, implementation, maintenance, and decommissioning) of information systems. The management must ensure information security requirements are incorporated into all third-

party contracts, to ensure NNSWA's information is protected against unauthorized access, data loss and outage.

The IT officer must implement and maintain an information security incident management process to respond to cyber-attacks. Security incidents must be managed in a manner that allows timely and accurate identification of, containment of, and remediation of security incidents. Before procurement, development of any new capabilities, or making any significant change to an IT system, the IT system owner must ensure that a risk assessment is conducted under the guidance of an IT representative. The assessment must focus on identifying risks associated with the reputation of NNSWA and the confidentiality, integrity and availability of NNSWA's data.

All users shall ensure that NNSWA information is not stored or processed by third-party digital service providers (including cloud services) unless it has been approved from the supervisor or IT department (e.g., Google Drive). It is the responsibility of all individuals to report information security incidents to info@nnswa.org.np . If it is determined that a security incident arose, in whole or in part, due to user noncompliance with applicable regulations, rules, policies or procedures, this may result in forfeiture of the privilege to use technology resources as well as administrative, disciplinary, or other legal action as applicable.

1.7 Hardware:

This policy provides users with guidelines for the selection and change of NNSWA IT hardware. Changes in technology are so rapid that it is impossible to draft specifications that remain unchanged for an extended period. As a result, the IT department formulates and revises IT standards and specifications quarterly to serve as a rolling benchmark for acquisition of related equipment.

f. Ownership:

NNSWA owns all IT hardware it procures, and the information contained therein.

g. Retention:

All IT hardware may replace after technical review of the organization. Any replacements will be made after proper justification. The IT department may revise the replacement cycle depending on the rate of technological advancement.

h. User privileges:

- NNSWA users cannot have more than one computer (e.g. a desktop and laptop). If users have a desktop, they can use a shared laptop for traveling or occasional home use.
- In consideration of the professional staff's need for mobility, at the time of replacement they can select a desktop or laptop (with docking station) as a new computer.
- This choice is not given to other users currently, as costing is prohibitive and the need for mobility is less critical. Exceptions for key support staff can be provided for the following justification.
- To address support, and shipping concerns, local procurement of IT hardware is encouraged if pricing does not exceed a 50% surcharge of standard unit cost.
- User owned hardware is not permitted to use wired network connections as this poses a security risk. Wireless connectivity is permitted where available.
- NNSWA is not responsible for the maintenance, support, or reimbursement of user owned hardware.

i. Accountability:

NNSWA users are responsible for the reasonable care of the hardware assigned to them. Should the loss or damage of the hardware be attributable to negligence on the part of the user, he/she will incur costs related to the repair or replacement of the equipment. Failure to do so may result in disciplinary action.

j. Security:

All NNSWA users are accountable for ensuring the integrity, privacy, and security of assets assigned to them. Laptops and other portable devices must be secured to prevent theft.

k. Ethical behavior and responsible Use:

NNSWA provides hardware for business operations and for performing daily work activities. Costs associated with personal use will be borne by the individual through issuance of a personal check to NNSWA. Commercial use of NNSWA hardware is strictly prohibited. Users may be subject to disciplinary action if found using hardware contrary to this policy.

1.8 Software:

The goal of this policy is to provide stable technology software solutions that appropriately address business needs. A lack of standards regarding what software can be installed on organizational devices, including desktop and laptop computers, can hinder provision of service. Controlling organizational software is not only a best practice for cost control, but also required for legal compliance. The Software Policy articulates what software is permitted on enterprise devices and who authorizes and carries out the installation task.

h. Ownership:

NNSWA owns all IT software procured utilizing its resources. It is forbidden to install NNSWA licensed software on computers not belonging to the organization.

i. Supported software:

Employees must use the licensed version of software after consulting the IT department of the organization. Details on currently supported versions of software can be found here:

Following is a general listing of supported software:

- Microsoft Windows (7, 8, 10 and 11) Professional versions
- Microsoft Office (Word, Excel, PowerPoint, Outlook)
- Google Apps (Gmail, Hangouts, Docs, Sheets, Slides)
- Google Chrome
- Mozilla Firefox
- Adobe Acrobat Reader
- Teams
    - Zoom
    - Meet and Skype, Another virtual platform.

Apart from some software that complies with partner, donor and government use, all software updates should be performed or set up by IT staff to ensure compatibility with systems and applications.

j. Prohibited software:

It is expressly forbidden to distribute or use computer programs for reasons such as scanning networks, intercepting information, or password capture unless specific authority is obtained from the IT section or management.

NNSWA users must comply with copyright laws and respect the intellectual property rights of others. It is therefore expressly forbidden for users to have possession of unlicensed software on NNSWA premises or, during carrying out their employment, use unlicensed software on NNSWA computers. Users of unauthorized copies of software will be disciplined as appropriate under the circumstances.

k. Shareware:

Shareware software is copyrighted software that is distributed freely through the Internet. Generally, the software is free to evaluate but continued, or commercial may require a license. Shareware software must be technically endorsed by the department head prior to installation by IT staff.

l. Purchase of software:

To purchase non-standard software costing over Rs 50,000 email approval must first be obtained from the IT Section. For software purchases costing over Rs 500,000, a formal request must be presented, and approval obtained from the Executive Director.

m. Accountability:

Users must not duplicate licensed software for use either on premises or elsewhere unless expressly authorized to do so. Users may not give software to third parties, including contractors. Users may use software on networks or on multiple machines only in accordance with applicable license agreements. Software must only be installed, modified, de-installed or deleted in accordance with agreed change management procedures, and must only be undertaken by authorized IT personnel.

n. Ethical behavior and responsible Use:

NNSWA provides software to staff to facilitate business operations and assist in performing daily work activities. Any costs associated with personal use will be estimated by IT section and borne by the individual through issuance of a personal check to NNSWA. Commercial use of NNSWA software is strictly prohibited. Users may be subject to disciplinary action if found using software contrary to this policy.

1.9 Email:

This policy provides users with technical guidelines for permitted use of the NNSWA email system and details how to ensure the system remains secure from unauthorized access. It also outlines email protocols to ensure information is shared within the organization in the most appropriate, systematic, and effective manner. This includes everyone with permanent, fixed, and temporary appointments, Special Service Agreements, interns, or other types of contracts. Users with a contract less than one month in duration are not entitled to a NNSWA email account. Anyone separating from the organization will retain access to their email address for a period of one month upon leaving. Exceptions in the interest of NNSWA may be authorized by the Administration. NNSWA email correspondence is considered an official form of communication.

h. Ownership

NNSWA owns its email system, messages generated or processed by the system including backup copies, and the information contained therein. Although users receive an individual email account, emails or its content and resources remain the property of the organization.

i. Retention

All emails sent and received by NNSWA are backed up and saved for a period of ten years. Emails can be recovered at the request of the user through the IT department of the organization.

j. Monitoring

NNSWA monitors the content of email to resolve problems, provide security, or investigate activities. Consistent with generally accepted business practices, NNSWA collects statistical data about its technology resources and technical staff monitor the use of email to ensure ongoing availability and reliability.

k. Accountability

Email messages are official communication. They should be treated in the same manner as other types of communication including handwritten, type-written, printed, photographed, or other formats of information. Users may be subject to loss of email privileges and or disciplinary action if found to be using email contrary to this policy.

l. Security

Users must maintain the confidentiality of passwords, regardless of the circumstances, and never share or reveal them to anyone. Electronically transmitted information travels through many networks, and many different computer connections. It is important to be aware that unless encrypted, email is not secure, and may be read by others. Users must contact the IT department with queries regarding the security and appropriateness of information sent via email.

m. Ethical Behavior and Responsible Use

NNSWA provides email to users to facilitate business communication and assist in performing daily work activities. Therefore, email users must practice ethical and acceptable behavior.

n. Email signature

Email accounts created for new staff automatically include the standard NNSWA email signature, including the NNSWAs Master Narrative, logo, and links to the NNSWA website and Facebook channels. The standard NNSWA email signature is automatically inserted in all outgoing messages sent to external (non-NNSWA) recipients.

In addition to the standard NNSWA email signature, all NNSWA personnel are required to insert their own personal signature in outgoing messages addressed to internal or external recipients. The signature should include full name, Job Position, Project Name, Organization name, Address, email address, contact number. The NNSWA Master Narrative and logo with tag line are the only graphic elements to be used in the email signature. Other quotes, images or personal information of any type are prohibited.

1.10 Server Back Up/Protection:

The purpose of this policy is to define the backup schedules for all the server groups and ensure server continuity to support the backup and restoration of archived information in the eventof a natural disaster, equipment failure, and/or accidental loss of files. The goals of this backup policy are outlined as follows:

- To safeguard the information assets of NNSWA.

- To prevent the loss of data in case of accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes
- To manage and secure backup & restoration processes and the media employed within these processes.

h. Staff Responsibilities and Accountability:

IT section is responsible for backing up user data stored on Organization servers. The IT department must designate a dedicated Backup Administrator as well as an alternate, who will work under the supervision of IT officer and will be responsible and accountable for backup and restoration management.

i. Backup Criteria:

The Backup Administrator must put in place procedures to create backup copies of all critical data stored on NNSWA servers. Critical data is defined as application source code, email data, and official documentation which is stored on servers. Methods are implemented for authorized users to gain access to the backup data quickly. These procedures are updated yearly to accommodate changes in policies or procedures at NNSWA. We must consider the following criteria in implementing the backup policy on a per system basis.

- **Selections:** what information is to be backed up on systems.
- **Priority:** relative importance of information for prioritizing backup jobs.
- **Type:** the frequency and amount of information backed up within a set of backup jobs.
- **Schedule:** the schedule to be used for backup jobs.
- **Duration:** the maximum execution time a backup job may take prior to its adversely affecting other processes.
- **Retention Period:** the period for which backup images created during backup jobs are to be retained.

j. Restore Request procedure:

All requests for restoration services must be submitted through the Supervisor. The Backup Administrator must complete all the restoration requests within one business week.

k. Off Site Backup:

NNSWA offices must maintain an offsite **secure** backup facility where critical data is stored. An acceptable offsite backup facility could be another agency, bank, etc…Preferred storage media forms are hard drives pen drives.

l. Defining what is to be backed up:

All data and software essential for the continued operation of all NNSWA services must be backed up.

In backing up information, all supporting material (e.g. programs, control files, and operating system software) required to process the information must also be backed up, although not necessarily with the same frequency as the data.

At the center office the Backup Administrator will determine what information to back up, in what form, and how often, in consultation with the IT department and the technical staff that are responsible for the specific data.

m. Types of data backup:

There are various procedures for backing up data which are listed below:

- Full data backup: With this procedure, all data requiring backup is stored on an additional data medium without consideration as to whether the files have been changed since the last backup. Therefore, this method requires a high storage capacity.
- Differential data backup: This procedure stores only the files that have been changed since the last full data backup. For restoration of data, the latest full data backup followed by the most recent differential backup, will suffice to restore the data.
- Depending on the degree of automation that is required and the storage location the Backup Administrator should select and implement the appropriate backup procedure. Automatic data backups are the first preference for all data backup procedures.
- It must be implemented in all cases possible by triggering a program at certain intervals. The manual data backup will be performed by the Backup Administrator only as needed.

n. Storage medium:

The Backup Administrator determines the appropriate media for backups considering the following criteria:

- The amount of time it takes to identify the data media necessary for backup and making them available to the system.
- The actual time required for restoring the data, which depends on the average time needed to access the data on the storage medium, the rate of data transfer, and the number of files involved.
- Storage capacity of the data media to ensure large volumes of data are being backed up effectively.
- The cost of data backup (cost of read/write devices, data media and time required for operations).
- The life and reliability of the data media should also be taken into consideration.
- The availability of requirements for faster access to data media for backup purposes, and for re-importing the relevant data from the backup data media.
- In the case where retention schedules call for deletion/erasure of data at specific times, the selected storage medium must allow this deletion.
- In case of confidentiality and integrity issues which prevent encrypted data, then consideration should be given to data media whose design and transport characteristics would allow their storage in locked vaults.

3. Data Protection Procedures:

The **Data Protection Procedures** ensures the adequate level of data protection as prescribed by relevant legal frameworks, including in countries that do not yet have adequate data protection laws. **Data protection Procedure** is meant to be a practical and easy to understand document to which all departments, stakeholders and relevant parties can refer to. **Data Protection Procedure** applies to all personal data that

IMPACT holds relating to identifiable individuals, meaning any information relating to an identified or identifiable individual.

2.10 SCOPE OF THE PRODUCER:

This 'Data Protection Policy' adhere all the rules and regulations of the Government of Nepal where the Act strives to protect the fundamental **right to privacy of every data** subject ("Individual"), such as privacy of body, family, residence, property, document, data, correspondence, and character, privacy of personal information through electronic means and protection of sensitive data. It imposes data protection and privacy obligations of individuals entrusted upon public bodies or entities. The Act deals with both personal information and sensitive personal information and identifies respective obligations for each.

2.11 GOVERNING LAW

Data protection and privacy matters in Nepal are governed by several different laws.

- Constitution of Nepal 2015
- Individual Privacy Act, 2075
- Individual Privacy Regulation, 2077
- Electronic Transactions Rules 2064 (2007)

2.12 APPLICABILITY OF THE Policy:

The Data Protection Policy is applicable during collection, storage, processing, use, analysis, and preservation of personal information of any individual residing in Nepal or individuals located in Nepal as per the Act of Government of Nepal.

Article 29 of the Constitution of Nepal ensures right to privacy and protection of personal information as a matter of fundamental right. With the view of giving effect (a) to the constitutional right to privacy of the matter relating to body, residence, property, document, data, correspondence and character of every person, (b) to manage the protection and safe use of personal information remained in any public body or institution and (c) to prevent encroachment on the privacy of every person, the **Individual Privacy Act, 2075** ("The Act") and the Individual Privacy Regulation, 2077 ("The Regulation") were enacted.

Furthermore, the provisions related to privacy and data protection are incorporated in the **Muluki Criminal Code, 2074**. The Act prohibits various conducts such as listening to or recording other's conversation, divulging confidential matter, taking photograph of any person without his/her consent, giving, or selling one's photograph to another without consent, opening letters or tapping conversation, breaching privacy through electronic means and unauthorized search of bodies or belongings of person.

2.13 PERSONAL INFORMATION:

Personal Information means the following information related to any person as stated in Government Act:

a) Caste, ethnicity, birth, origin, religion, color, or marital status,
b) Education or academic qualification,
c) Address, telephone, or address of electronic letter (email),
d) Passport, citizenship certificate, national identity card number, driving license, voter identity card or details of identity card issued by a public body,

e) A letter sent or received by an individual mentioning personal information,
f) Thumb impressions, fingerprints, retina of eye, blood group or other biometric information,
g) Criminal background or description of the sentence imposed upon individual for a criminal offence or service of the sentence,
h) A matter of opinion or view expressed by professional or expert in the process of any decision.

2.14 COLLECTION OF PERSONAL INFORMATION:

The Act permits only an official authorized under law ("Authorized Person") or the person permitted by such official to collect, store, protect, analyze, process, or publish the personal information of any individual. Therefore, the Authorized Person must (a) fully inform the individual regarding the purpose for which the information is collected and (b) obtain consent from such individual.

While collecting information, the individual must be provided with the following information:

a) Time of collecting information,
b) Content of information,
c) Nature of information,
d) Objective of collecting information,
e) Method and process of testing information,
f) Certainty of the matter of maintaining privacy of the collected information, and
g) Matters include the protection of the collected information.

2.15 PROCESSING/USE OF PERSONAL INFROMATION:

Since the Act permits the personal information collected by public entity to be processed or used upon obtaining consent of an individual, the data so collected can be used only for the purpose for which such data has been collected. Using information to inflict or insult in the personal life of an individual is strictly prohibited. The public entity must make appropriate arrangements against unauthorized access likely to occur to personal information, or against the possible risk of unauthorized use, change, disclosure, publication, or transmission of such information.

Furthermore, this policy mandates consent of the guardian or curator of the minor for using information relating to the privacy of minors, persons of unsound mind provided that it benefits to the interest of such persons.

However, **the personal information so collected by public entity can be processed without consent of an individual in the following conditions:**

- If there is a provision incorporated for collecting such information by the Authorized Person under the existing laws,
- If such information is collected during investigation, prosecution of criminal offence or under the order of the Court, or
- If it is collected or processed for the maintenance of national security or peace and order.

In addition, this policy prohibits public entities to process sensitive information unless (a) required for diagnosis, treatment, management and delivery of health services or emergency rescue to an individual and (b) if an individual himself/herself makes such information public.

2.16 RETENTION OF PERSONAL INFORMATION:

The Act imposes obligations upon an Authorized Person to collect, store, protect, analyze, process, retain or publish the personal information of any individual. So, this policy will fully comply with the provisions in the Act.

2.17 TRANSFER OF DATA:

The term "transfer" indicates **transferring of personal information** to the third party thereby requiring consent from a concerned individual. Pursuant to the Act, the consent of an individual is sufficient for transferring the data. The Act prohibits disclosing or transferring of personal data of an individual without obtaining consent from such an individual:

- Details relating to health examination,
- Details relating to property and income generation,
- Details relating to employment,
- Details relating to family matters,
- Biometric details and thumb impression,
- Signature or electronic signature,
- Details relating to political affiliation and election,
- Details relating to business or transaction.

2.18 RESPONSIBILITY OF THE PUBLIC ENTITY:

The Act puts obligation upon public entities to **protect and preserve the personal information** that has been collected or remained under the responsibility or control of such entity. The information collected by a public entity cannot be transferred or disclosed to the third party without obtaining consent of an individual.

The Act has mandated public entity to make appropriate arrangements against unauthorized access likely to occur to personal information, or against the possible risk of unauthorized use, change, disclosure, publication, or transmission of such information. Furthermore, the sensitive personal information collected by a public entity cannot be processed or used. In addition to this, the Act also aims at regulating public entity to correct the collected information upon submitting sufficient evidence by an individual to why such information has been wrong or upon providing justification for his/her claim. However, such application is not entertained if an individual has already taken advantage of the facilities based on the information provided.

2.19 RIGHTS OF INDIVIDUALS:

a) The right of access and being informed.

The Act provides that an Authorized Person who collects, stores, processes, analyzes and protects the personal information to inform the individuals regarding the subject matter of collected information and the purpose of collecting such information. The individuals have the right to confirm if the Authorized Person has made necessary arrangements against unauthorized access likely to occur to personal information, or against the possible risk of unauthorized use, change, disclosure, publication, or transmission of such information as provided in section 25 of the Act.

Likewise, the Act grants individuals the right of access to information such as time, nature, content, objective, method of information collection.

b) The right of rectification:

If personal information remaining under the responsibility, protection or control of any public entity is either wrong or is not based on fact, the Act provides the individual an individual to file an application to correct such information. The Act requires a public entity to communicate the decision of rectification of personal information in case an individual submits notice of rectification along with the relevant evidence substantiating the rectification. However, such applications can only be filed before taking advantage of the facilities based on the information provided. This right of rectification is limited to the personal information under the control of a public entity.

c) Right to restriction of processing

Upon obtaining consent from an individual, the Act and Regulation do not provide for specific provision relating to restriction of processing.

2.20 BREACH OF DATA:

The right to privacy is a fundamental right and violation of which would amount to criminal offence. The aggrieved party can initiate the criminal proceeding either as a private party or a state party for violating provisions of the Act. The offences such as collection of personal information by any person other than the Authorized Person, collection of personal data without mentioning the purpose of collecting such information, disclosing the personal information without his/her consent are criminalized by the Act. For acts amounting to offences as stipulated under the Act, punishment of imprisonment for a term not exceeding three years or fine not exceeding thirty thousand rupees or both will be applicable. Additionally, the party aggrieved by an offence can claim compensation for any damage, loss or pain incurred. The court can grant reasonable compensation to the aggrieved party if the court is of the opinion that such damage, loss, or pain is incurred.

If any member of Staff, or other person learns of a suspected or actual Personal Data Breach, it must be reported to **info@nnswa.org.np** immediately. The report should include as many details of the incident as possible, including date and time of the breach (if known), the nature of the information concerned, and how many individuals are involved.

2.21 IMPLEMENTATION OF THE POLICY:

This policy has been endorsed by the Executive Board and approved by the General Assembly on November 3rd 2023 and comes into effect immediately. The policy would be periodically reviewed and updated as and when necessary.

The policy endorsed by Executive Board Meeting:

Maya Devi Sarki -President

Rupa Kausal Pariyar -Secretary General

Suresh Kumar Palpali - Secretary

Reshma Rana - Member

Gehendra Nepali - Member

Ratan Damai -V. President

Kabita Bhatt -Treasurer

Roshan Lal Chaudhary - Member

Babita Sunar - Member

Arati Urau - Member

Date: November 3rd 2023

Official Stamp
NNSWA
Central Office
Kanchanpur

Counter Signature:

Ashok Bkram Jairu
Executive Director/
Founder President