IT & Data Privacy Policies

YOUNG POWER IN SOCIAL ACTION
* BANGLADESH *

Young Power in Social Action (YPSA)
www.ypsa.org

IT & Data Privacy Policies

Young Power in Social Action (YPSA)
An Organization for Sustainable Development
Organization in Special Consultative Status with the United Nations
Economic and Social Council (UN ECOSOC)

4 decades in development partnership | Since 1985

Head Office (At Commercial Capital City)

Young Power in Social Action (YPSA)
House # 10 (F) P, Road # 13, Block-B, Chandgaon R/A, Chittagong - 4212,
Bangladesh.
Tel: +8802334471690, Cell: +8801711825068
E-mail: info@ypsa.org , ypsa_arif@yahoo.com

Dhaka office (At Capital City)
Young Power in Social Action (YPSA)
House # 12/Umo/1 (Ground floor), Road# 02, Shyamoly, Dhaka- 1207,
Bangladesh.
Tel:+88-02-8142351, Cell no: +8801818578790
E-mail: ypsadhaka@gmail.com
website: www.ypsa.org , Facebook: www.facebook.com/YPSAbd

ইয়ং পাওয়ার ইন সোশ্যাল এ্যাকশন (ইপসা)
স্থায়ীত্বশীল উন্নয়নের জন্য সংগঠন

Young Power in Social Action (YPSA)

An Organization for Sustainable Development

[Organization in Special Consultative Status with the United Nations Economic and Social Council ECOSOC]

YPSA
is a non-governmental voluntary non Profit non Political Organization for Sustainable Development registered with various departments of Bangladesh Government. YPSA established in 1985 being inspired by the spirit of International Youth Year declared by the UN. YPSA works in close co-operation with Government, INGOs & UN agencies. YPSA awarded International Youth Peace Prize 1999 for it's outstanding social development Programmes.

Vision
YPSA envisions a society without poverty where everyone's basic needs and rights are ensured.

Mission
YPSA exists to participate with the poor and vulnerable population with all commitments to bring about their own and society's sustainable development

Core Values

- Patriotism and commitment to national interest, sovereignty and national pride
- Justice, transparency and accountability
- Mutual respect and gender friendliness
- Quality and excellence
- Humility and confidence
- Respect for diversity
- Support for environment and ecology

web site:
www.ypsa.org

Ref: YPSA/HO/307-1/2024

Date: 04 February 2024

OFFICE OF MEMORANDUM

Subject: YPSA IT and Data Privacy Policies

The set of policies on the above subject has been approved by the Executive Committee Meeting on 02 February, 2024. The policies will be in effect from March 1, 2024.

We record our gratitude and thanks to the General Council and Executive Committee members of YPSA for providing necessary briefing and guidelines during finalizing this policy. Thanks to the YPSA staff for their suggestions during developing the policies.

Our heartiest thanks to our Donors/Partners for their technical support for developing the policies.

I request everyone associated with YPSA to adhere these policies and contribute to its development.

(Md. Arifur Rahman)

Chief Executive, YPSA

YOUNG POWER IN SOCIAL ACTION ★BANGLADESH★

YOUNG POWER IN SOCIAL ACTION * BANGLADESH *

Contents

YOUNG POWER IN SOCIAL ACTION
* BANGLADESH *

1. Introduction

The YPSA IT and Data Privacy Policies provides a guideline for selection and uses of IT gadgets and how personal/project data collected, handled and stored to meet the organizations data protection standards. YPSA will comply national data and IT laws and regulations. Therefore from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures. Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

YOUNG POWER IN SOCIAL ACTION * BANGLADESH *

2. Objectives

Objectives of IT and Data privacy policies are;

- **Safeguarding Confidentiality**: Protecting sensitive information from unauthorized access or disclosure, ensuring the confidentiality of data.
- **Ensuring Data Integrity:** Maintaining the accuracy and reliability of data by implementing measures to prevent unauthorized modification or deletion.
- **Promoting Compliance:** Adhering to relevant laws, regulations, and industry standards regarding data protection and privacy.
- **Minimizing Risk:** Identifying and mitigating potential risks to data security, including cyber threats, breaches, and data loss incidents.
- **Fostering Trust:** Building trust among stakeholders by demonstrating a commitment to respecting individuals' privacy rights and handling their data responsibly.
- **Enhancing Accountability:** Establishing clear roles and responsibilities for managing and protecting data, holding individuals and teams accountable for compliance with policies and procedures.
- **Facilitating Responsiveness:** Ensuring the organization can respond effectively to data privacy incidents, inquiries, and requests from individuals regarding their personal information.

3. Definitions

Key policy definitions can be found in Annex 2 of this Policy

4. Scope of IT & Data Privacy Policies

These Policies are coverage the use and purchase of hardware and software (IT gadgets), portable devices use guideline, information technology security policy, data privacy policy, website and social media policy, emergency management of information technology. These policies are applied to all employees.

5. Policy for Purchase Hardware

5.1 Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the organization to ensure that all hardware technology for the organization is appropriate, value for money and where applicable integrates with other technology for the organization.

YOUNG POWER IN SOCIAL ACTION • BANGLADESH •

5.2 Procedures

5.2.1 Request for Hardware

All hardware, must be approved or suggested by supervisor/web manager/relevant technical person prior to the purchase or hire of such hardware (computer, laptop, mobile/tab, camera, portable hard disk, server etc.).

5.2.2 Purchase of Hardware

According to Organization Procurement Policy

6. Policy for Purchase of Software

6.1 Purpose of the Policy

This policy provides guidelines for the purchase of software for the organization to ensure that all software used by the organization is appropriate, value for money and where applicable integrates with other technology for the organization. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

6.2 Procedures

6.2.1 Request for Software

All software, must be approved or suggested by supervisor/web manager/relevant technical person prior to the use or download of such software. The required software will be rational and appropriate.

6.2.2 Purchase of software

According to Organization Procurement Policy

7. Policy for Use of Software and Hardware

7.1 Purpose of the Policy

This policy provides guidelines for the use of software and hardware for all employees within the organization to ensure that all software and hardware use is appropriate.

7.2 Appropriate Usage

Prior to the use of software and hardware, the employee must receive instructions (training if required) to use software and hardware appropriately. This will be the responsibility of supervisor/admin/web manager. Employees are discouraged to insert unauthorized pen drive or portable disk onto the organization computer hardware without scanning virus. The hardware can be taken home (if necessary). But it has to be taken care of and safety must be ensured. The inappropriate use of software or hardware is not condoned within this organization and authorized will undertake disciplinary action where such event occurs.

8. Bring Your Own Device/Portable Device Policy

We acknowledge the importance of mobile technologies in improving organization communication and productivity. This policy should be read and carried out by all staff.

8.1 Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and other types of mobile devices for organization purposes. All staff who use or access YPSA's technology equipment and/or services are bound by the conditions of this Policy.

YOUNG POWER IN SOCIAL ACTION
★ BANGLADESH ★

8.2 Procedures

The following personally owned mobile devices as notebooks, smart phones, tablets, iPhone are approved to be used for organization purposes and personal purposes. Employees when using personal devices for organization or personnel reasons, it is his/her responsibility to ensure its safety. Portable devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away. Portable devices should be carried as hand luggage when travelling.

9. Information Technology Security Policy

9.1 Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the organization to ensure integrity, confidentiality and availability of data and assets.

9.2 Physical Security

For all computer/laptop, servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access. All security and safety of all portable technology will be the responsibility of the employee who has been issued with the IT assets. In the event of loss or damage of IT assets, the employee should report it to admin/web manager/supervisor or dedicated reporting channel in immediately. The respective concern will assess the security measures undertaken to determine if the employee will be required to reimburse the organization for the loss or damage.

9.3 Information Security

All insert relevant data is to be backed-up. It is the responsibility of users to ensure that data back-ups are conducted monthly and the backed-up data is kept in portable hard disk/cloud or any safety places. Information backups can be more frequent depending on the project or department's context. Given emphasis cloud on data storage and IOT/AI in data analysis. All technology that has internet access encourage to have anti-virus software installed. Or, use virus protection enabled operating system. All information used within the organization is to adhere to the privacy laws and the organization's confidentiality requirements.

9.4 Technology Access

Every employee will be issued with a unique identification code to access the organization technology/laptop/computer/server and will be required to set a password for access. Each password is to be alpha numeric and is not to be shared with any employee within the organization. User is responsible for the issuing of the identification code and initial password. Where an employee forgets the password or is 'locked out' then user is authorized to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password. If an employee leaves, he/she will tell the admin/supervisor his/her computer/laptop password and hand over the laptop/computer to him.

YOUNG POWER IN SOCIAL ACTION * BANGLADESH *

10. Data Privacy Policy

10.1 Purpose of the Policy

Data Privacy Policy is a critical document that outlines an organization's commitment to protecting the confidentiality, integrity, and security of personal data entrusted to it. It delineates how the organization collects, processes, stores, and shares personal information while adhering to relevant data protection laws and regulations. YPSA has a dedicated information officer who is responsible to provide organization information to user. Moreover, data storage responsibilities may be controlled by departments wise.

10.2 Principles of Data Privacy Policy

Principle-01: Purpose and Manner of collection

- Personal data must be collected in a fair way;
- Data subjects must be notified of the purpose;
- Data collected should be necessary but not excessive;

Principle-02: Accuracy and Duration of Retention

Personal data must be accurate and should not be kept for a period longer than is necessary to fulfil the purpose for which it is used. Generally, YPSA will follow the local law and donor guidelines in regards of retention of data. Departmental/subjective policies will be applicable on retention of departmental data. For instance, the financial policy will be followed in relation to the retention of financial records or data.

Principle-03: Use of Data

Personal data must be used for the purpose for which the data is collected or for a directly related purpose.

Principle-04: Data Security

A data user must take practical steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.

Principle-05: Openness and Transparency

A data user must make personal data policies and practices known to the public, regarding the types of personal data it holds and how the data us used.

Principle-06: Access and Correction

A data subject must be given access to his/her personal data and allowed to make corrections if it is inaccurate.

10.3 Reporting and Compliances

Data security incidents and breaches shall be promptly reported to the designated reporting channel as hotline and designated email. An incident response team shall be established to investigate and respond to security incidents according to organization case management policy. YPSA will comply with relevant data protection laws and regulations in Bangladesh.

YOUNG POWER IN SOCIAL ACTION
* BANGLADESH *

11. Website and Social Media Policy

11.1 Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the organization website and social media. Ensure that all website/social media content aligns with the mission, values, and goals of the YPSA.

11.2 Procedures

11.2.1 Website/Social Media Register

The website register, social media info must record the following details:

- List of domain names registered to the organization
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting
- Store the user's name and password of social media in properly and securely (keeping register or safe place).
- The keeping the register up to date will be the responsibility of web manager/admin. He will be responsible for any renewal of items listed in the register.

11.2.2 Social media/website content Guideline

- Determine the appropriate tone and voice for communicating with the audience;
- Develop content that is visually appealing, concise, and easy to understand;
- Use high-quality images, videos, and graphics to enhance engagement;
- Ensure that all content is accurate, credible, and fact-checked before publishing.
- Avoid using language or imagery that may be offensive, discriminatory, or insensitive.
- Respect copyright and intellectual property rights when using third-party content.
- Respond promptly to comments, messages, and mentions from followers.
- Foster meaningful conversations and interactions with the audience.
- Act swiftly and transparently to address any issues and mitigate reputational damage
- Ensure that all content complies with applicable laws and regulations, including data protection and privacy laws.
- Employees and volunteers are encouraged to use social media responsibly to promote the organization's work.
- Opinions expressed by the employees on their personal social media account are strictly their own and not necessarily those of YPSA.
- The guidelines mentioned in the circular regarding ensuring digital security and use of social media should be followed.

12. Email and Internet Usage Policy

12.1 Purpose of the Policy

The Email and Internet Usage Policy is a set of guidelines and rules established by an organization to regulate the use of email and internet resources by its employees. This policy outlines the acceptable and unacceptable behaviors related to the use of company-provided email accounts, internet access, and other online resources.

YOUNG POWER IN SOCIAL ACTION * BANGLADESH *

12.2 Procedures

Employee while joining the organization, a mail ID should be opened with YPSA name attached. Until the organization's mail server becomes available, employees can use open mail IDs (gmail, yahoo) or any free mail server. If use free mail server then must attached YPSA in mail ID, such as employee last name with attached YPSA. The web manager/admin will help on opening employee mail ID (if required). Employees are suggested to use this mail for official work. Employee while leave the organization, he/she must close/deactivate the mail id (in regards of open mail server) and give promise not to use this mail again. And if the mail id is using the domain of the organization, then the web manager/admin will deactivate this id. Employee cannot use this official mail for any malpractice. In regards of using official internet, employee cannot misuse it and not carrying/downloading/uploading any illegal contents.

13. Emergency Management of Information Technology

13.1 Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the organization.

13.2 Procedures

- Where there is failure of any of the organization's hardware and software this must be referred to admin/web manager/manager immediately.
- It is the responsibility of admin/web manager to take action and effort in the event of IT hardware and software failure.
- Immediately notified Point of Service (POS provider).
- The concerned person (admin/web manager) shall contact the concerned supplier (POS) and arrange for the device repair or maintenance (if have warranty period).

13.3 Security breach

- In the event that the organization's information technology and data privacy and other relevant possible security breaches are happened then immediate reported to admin or organization reporting mechanism/channel.
- HRMD&D is responsible to deal the possible security breaches and minimize disruption to organization operations.

14. Policy review

This policy is reviewed at minimum every five years. The review process will seek contribution and feedback from personnel and external stakeholders. YPSA is committed to reviewing the IT & Data Privacy Policies and Procedures following incidents and near misses. Changes may also be made to the policy following key legislative change or emerging best practice standards.

YOUNG POWER IN SOCIAL ACTION * BANGLADESH *

Annexure:

Definitions

Consent

Consent means, in light of the information provided to the individual data subject, any freely given.

Data

Data refers to raw facts, figures, or statistics collected, stored, and processed for various purposes. It can take various forms, including text, numbers, images, audio, and video.

Personal Data

Personal data means any information relating to an identified or identifiable individual ('data subject'). An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, phone number, audiovisual materials, location data, an online identifier The definition of what constitutes personal data is contextual and expanding particularly due to enhancements in technology and methods for identifying individuals.

Personal data breach

Personal data breach means a breach of security leading to the accidental or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability of personal data that is unencrypted or can be decrypted. A breach does not exist where access is the result of disclosure or access consistent with official functions.

Personal data transfer

Personal data transfer means any action that makes personal data accessible or otherwise available to another party, other than the data subject, regardless of the media and format (electronically or physically).

Data Subject

Data subject means an individual whose personal data is subject to processing under this Policy.

Data User

Data user is a person who, either alone or jointly or in common with persons, control the collection, holding, processing or use of data

Information technology (IT)

Information technology (IT) refers to the broad field that encompasses the use of computers, telecommunications, and other electronic devices to store, retrieve, transmit, and manipulate data or information.

Illegal content

Illegal content on the internet refers to any material that violates local, national, or international laws and regulations.

YOUNG POWER IN SOCIAL ACTION
★BANGLADESH★

Software

Software refers to a collection of instructions, programs, or data that enable computers and other electronic devices to perform specific tasks or functions. It includes applications, operating systems, utilities, and other programs that control hardware and facilitate user interactions.

Hardware

Hardware refers to the physical components of a computer system or electronic device

Portable Devices

Portable devices are electronic gadgets or tools designed for easy mobility and use while on the go. These devices are typically lightweight, compact, and battery-powered, allowing users to carry them around conveniently. Examples of portable devices include smartphones, tablets, laptops, portable media players, handheld gaming consoles, and wearable devices like smartwatches and fitness trackers.

Website

A website is a collection of web pages and related content that is typically identified by a common domain name and accessible over the internet through a web browser. Organization has a central website, also have some project or service-based websites.

Social Media

Social media refers to online platforms and websites that allow users to create and share content, interact with other users, and participate in virtual communities. Examples of social media platforms include Facebook, Twitter, Instagram, LinkedIn, YouTube, and TikTok. Organization has central web page, also have some project or service-based pages, groups.