Health Education and Development Society
(HEADS)

Information Technology (IT) Policy

Health Education and Development Society (HEADS)

Abstract

This Information Technology (IT) Policy outlines the Health, Education and Development Society's (HEADS) standards for secure, ethical, and efficient use of its IT infrastructure. It sets clear protocols for data confidentiality, system integrity, authorized access, and cybersecurity compliance across all levels of operation. Covering areas such as acceptable use, password protection, internet access, data privacy, incident response, and third-party compliance, the policy ensures robust protection of digital assets and alignment with regulatory requirements. Updated in January 2025, this policy reinforces HEADS' commitment to secure technology use, data protection, and responsible digital governance in all operational environments.

www.heads-ngo.org

(HEADS)

Background:

Health, Education and Development Society (HEADS), is a non-profit, non-political and non-governmental organization registered in Pakistan under the Societies Act 1860. Since its establishment in 2013, HEADS has been actively engaged in the developmental and humanitarian sectors. The organization is led by a dedicated Board of Governors (BoG), consisting of professionals with diverse educational backgrounds and capabilities. HEADS operate under a comprehensive set of policies designed to ensure transparency, accountability and efficiency in its systems and operations. HEADS Currently registered in the Islamic Republic of Afghanistan, and established an office in the capital city, Kabul.

Throughout its history, HEADS has worked closely with communities and various stakeholders, addressing a wide range of issues, including but not limited to Education, Health, Protection, Livelihoods, Community Infrastructure (CPIs), Shelter and Settlement, Community Development, Institutional Capacity Building, Research, Gender Equality, Legal Counselling, Referral Mechanisms, Social Accountability, Right to Information, and Governance.

In addition to these programmatic areas, HEADS place a strong emphasis on cross-cutting themes, including social mobilization, gender mainstreaming, inclusion, and resilience in all its core programs. These themes reflect the organization's commitment to addressing the holistic needs of communities and promoting sustainable development.

Vision: Every Individual regardless of background or circumstances enjoy equal opportunities and rights with dignity.

Mission: Empowering Communities through strategic investment in human capital and institutional capacity development, raising sustainable development at the grassroot level.

Objectives:

- Support and develop replicable models and strategies for sustainable human resource development through skills development initiatives.
- Network and collaborate with the Govt. Departments, NGO's, CBO's, WOs and international agencies/donors for sustainable development.
- Support initiatives for sustainable community-based gender sensitive development with particular focus on; Human and institutional Development, Natural Resource Management, Drinking Water Supply, Environmental Sanitation, Education, Agriculture, Health & Nutrition, Disaster Management and Micro Credit & Enterprise.
- Create economic and recreational opportunities for youth through skill enhancement programs for peace promotion.
- Enable equitable access to quality education and healthcare, raising holistic community development and well-being.
- Promoting Social Inclusion and Empowerment;
- Strengthen Resilience to Climate Change and Environmental Degradation.
- Advocacy for Peace, Human Rights, and Social Justice.
- Building Disaster Resilience and Preparedness

Introduction

HEADS is committed to maintaining the highest standards of information security, data protection, and responsible use of IT resources. This policy establishes the framework for ensuring the confidentiality, integrity, and availability of IT systems while aligning with regulatory compliance and organizational best practices.

Key Principles

To ensure effective IT governance, HEADS follows fundamental principles that guide the responsible use of IT resources. These principles include maintaining confidentiality, ensuring data integrity, providing availability, and enforcing accountability to prevent security threats and operational risks.

- **Confidentiality:** Protecting sensitive information from unauthorized access.
- **Integrity:** Ensuring data accuracy and preventing unauthorized modifications.
- **Availability:** Ensuring IT resources are accessible when required.
- **Accountability:** Holding individuals responsible for their use of IT resources.

Scope

This policy applies to all employees, contractors, consultants, vendors, and any third parties who have access to HEADS' IT infrastructure. It covers all digital assets, including hardware, software, networks, cloud services, and data storage systems.

Acceptable Use Policy (AUP)

The appropriate use of IT resources is essential for maintaining security and efficiency. Employees must use IT systems solely for authorized professional purposes, following security protocols, legal requirements, and internal guidelines to prevent misuse.

General Use

To ensure the responsible use of IT resources, users must:

- IT systems should only be used for professional and authorized activities
- Users must ensure compliance with security protocols and legal obligations.
- Keep login credentials confidential.
- Avoid accessing inappropriate content or using unauthorized software.
- Unauthorized access or modification of IT resources is strictly prohibited.
- Follow email and internet usage guidelines.

Personal Use

While limited personal use of IT resources is permitted, it should not disrupt professional duties or compromise security. Employees must refrain from accessing restricted content, excessive bandwidth usage, or engaging in activities that might create vulnerabilities in HEADS' IT systems.

- Limited personal use of IT resources is permitted if it does not interfere with work.

- Excessive bandwidth consumption or accessing inappropriate content is forbidden.
- Personal use must comply with HEADS' security policies to prevent vulnerabilities.

Passwords

Strong password management is critical to ensuring system security. Employees must create complex passwords, update them periodically, and enable Multi-Factor Authentication (MFA) for accessing sensitive systems to minimize the risk of unauthorized access.

- Users must create strong passwords with a mix of letters, numbers, and symbols.
- Passwords should be changed periodically and not shared with others.
- Multi-Factor Authentication (MFA) is mandatory for accessing critical systems.

Internet Access

Internet access must be used responsibly, ensuring compliance with security policies. HEADS monitors internet usage to prevent access to malicious websites, unauthorized downloads, and other activities that may pose cybersecurity threats.

- Internet access is monitored to ensure security and compliance.
- Downloading unauthorized software or accessing restricted websites is prohibited.
- Employees must use the internet responsibly, ensuring adherence to cybersecurity policies.

Specific Privacy Policy

HEADS prioritizes the protection of user data and ensures compliance with data privacy laws. The organization implements stringent security measures to collect, process, and store personal data securely while maintaining transparency in its privacy practices.

- Collecting minimal personal data necessary for operational purposes.
- Ensuring encrypted storage and secure handling of sensitive information.
- Providing users with transparency on data processing practices and rights.
- Complying with data protection regulations and conducting periodic privacy audits.

Data Protection

HEADS is committed to safeguarding personal and sensitive information. The following measures ensure data security:

- **Encryption:** Sensitive data must be encrypted during transmission and storage.
- **Access Control:** User privileges are assigned based on the principle of least privilege.
- **Data Retention:** Personal data will be retained only as long as necessary for operational or legal purposes.
- **Compliance:** Adherence to national and international data protection regulations (e.g., GDPR).

Cybersecurity & Threat Management

HEADS employs proactive cybersecurity measures, including firewalls, antivirus protection, phishing awareness training, and regular security audits. Employees are expected to remain vigilant against potential cyber threats and follow established security protocols. To mitigate risks, the following security controls are in place:

- **Firewall & Antivirus:** All systems must have updated security software.
- **Phishing Awareness:** Employees must complete cybersecurity training to recognize phishing threats.
- **Multi-Factor Authentication (MFA):** Enforced for access to critical systems.
- **Regular Security Audits:** IT systems undergo periodic vulnerability assessments.

Incident Response & Reporting

A robust incident response framework is in place to detect, respond to, and mitigate security threats. Employees must report any IT-related security incidents immediately to the IT department to ensure prompt action and prevent further risks.

- Any security incident must be reported immediately to the IT department.
- The IT team will investigate and mitigate threats following an incident response plan.
- Users must avoid taking unauthorized corrective measures to prevent data loss.

IT Asset Management

Effective management of IT assets is crucial for operational security. This section details the processes for documenting, tracking, and handling IT equipment, including policies for returning assets upon employee termination.

- All IT assets must be documented, labeled, and managed centrally.
- Employees must return IT equipment upon resignation or termination.
- Unauthorized hardware and software installations are prohibited.

Third-Party & Vendor Compliance

HEADS requires third-party vendors and external partners to comply with IT security policies. Data sharing agreements must be in place to ensure that any external access to HEADS' IT systems does not compromise security or confidentiality.

- Vendors accessing HEADS' IT systems must comply with security policies.
- Third-party data sharing must be governed by legally binding agreements.

Information Ownership

HEADS recognizes that IT assets, including data and infrastructure, are critical to its operations and must be protected. This section outlines the roles and responsibilities of various stakeholders, including IT personnel, users, and management, in ensuring proper ownership, security, and compliance.

IT Department

- Oversee the security, integrity, and availability of IT systems.
- Implement and enforce cybersecurity protocols, including firewalls, antivirus software, and monitoring systems.
- Conduct regular security audits and vulnerability assessments.

- Provide IT support, troubleshooting, and training to employees.
- Respond to and mitigate IT security incidents following the incident response plan.

Employees and Users

- Adhere to the IT policy and ensure responsible use of IT resources.
- Maintain strong passwords and enable Multi-Factor Authentication (MFA) where required.
- Report any suspected security incidents, phishing attempts, or data breaches immediately.
- Avoid unauthorized software installations, sharing sensitive information, or engaging in activities that compromise IT security.

Management

- Ensure that IT policies align with HEADS' strategic goals and compliance requirements.
- Support the IT Department in enforcing security protocols and addressing non-compliance.
- Review and approve changes or updates to the IT Policy as required.

Infrastructure, Security, and Compliance Manager

- Ensure that all IT systems, services, and storage solutions meet security and compliance standards.
- Perform regular security checks, updates, and system performance monitoring.
- Evaluate third-party vendors and service providers for IT security risks.
- Maintain and monitor data breach prevention systems.

Data Protection Officer (DPO)

- Ensure compliance with data protection regulations and privacy laws.
- Conduct audits on data handling, storage, and access controls.
- Respond to data subject access requests and oversee data privacy measures.
- Manage incident response in case of data breaches and ensure timely reporting.

Third-Party Vendors and Contractors

- Comply with HEADS' IT security policies and data protection guidelines.
- Ensure that any IT services provided align with contractual security and privacy standards.
- Report any security vulnerabilities or incidents related to HEADS' IT infrastructure.

Monitoring & Compliance

To maintain security and compliance, HEADS conducts regular audits of IT systems, monitors user activity, and enforces policies. Violations of IT policies may result in disciplinary actions, including restricted access or other corrective measures.

- **IT System Audits:** Regular audits ensure compliance with security standards.
- **User Activity Monitoring:** Systems may be monitored for security and compliance purposes.
- **Policy Enforcement:** Non-compliance may result in disciplinary action, including access revocation.

Policy Amendments & Review

HEADS

To keep pace with technological advancements and regulatory changes, HEADS periodically reviews and updates its IT policies. Employees will be informed of any changes, and compliance will be strictly enforced. This policy is subject to periodic review and amendments by the IT Department and Executive Management. Changes will be communicated to all users, and compliance will be enforced accordingly.

Effective Date & Acknowledgment

This policy takes effect immediately upon approval. All employees must acknowledge and adhere to the policy, confirming their understanding and commitment to maintaining IT security standards at HEADS. This revised version ensures clarity, compliance, and adherence to best IT security practices at HEADS.

BOD Meeting Minutes

Date: January 06, 2025

Participated by:

Raza Ullah Jan	Executive Director
Uzma Amin	Chairperson Board
Samina Khanam	Board Member
Nawaz Ali Shah	Board Member
Amabareen Banori	Board Member
Muhammad Jidran	Board Member
Abid Ali	Board Member
Tahira Nasreen	Board Member
Sayed Ali Shah	Director Program
Asif Ali	Director Finance
Ramsha Khan	HR Officer

Agenda Items:

- Change in Leadership position
- Formation of the Annual Report, Annual Budget, and Strategic Plan.
- Completion of the NDRMF Capacity Improvement Action Plan.
- Processing for Charity Commission in Balochistan and Khyber Pakhtunkhwa.
- Revision of HEADS policies.
- Renewal of Society Act Registration for 2025.

Proceedings & Outcomes:

The meeting commenced with the recitation of the Holy Quran, followed by a formal welcome note delivered by the Chairperson, Ms. Uzma Amin, and the Executive Director, Mr. Raza Ullah Jan. The discussions focused on the agenda items and organizational improvements.

- The Board decided to shift Mr. Raza Ullah Jan from the position of Chairperson of the Board of Directors (BOD) to Executive Director of HEADS, following the resignation of Ms. Samina Khanam from the role of Executive Director. Ms. Khanam has now joined the Board as a Board Member. Additionally, Dr. Uzma Amin has been appointed as Chairperson of the Board, effective immediately.
- The Board emphasized the importance of preparing Annual Report/ Annual Budget and Strategic Plan to assess the organization's current standing and plan strategically for the upcoming year.
- As HEADS has been conditionally accredited by the National Disaster Risk Management Fund (NDRMF) for six months, the Board reviewed the shared Capacity Improvement Action Plan. It was decided to prioritize its completion within the stipulated timeframe, recognizing this as a crucial opportunity for the organization.

- The Board agreed to initiate the process for Charity Commission registration in Balochistan. Police verification for the Charity Commission in Khyber Pakhtunkhwa will be expedited to obtain the certification promptly.
- A comprehensive review of organizational policies was conducted. The Board proposed and approved necessary amendments to align with current needs and best practices.
- It was noted that the Society Act Registration expired in December 2024. The Board resolved to apply for its renewal for 2025 without delay.

The meeting concluded with a thorough review of the agenda items, ensuring they aligned with the organization's strategic objectives. The Board expressed optimism about the successful execution of the discussed initiatives. The Chairperson concluded the meeting with a vote of thanks.

Signed on this Monday January 06, 2025 by authorized signatory.

Dr. Uzma Amin
Chairperson Board

Ms. Samina Khanam
BOG Member

Mr. Nawaz Ali Shah
BOG Member

Mr. Abid Ali
BOG Member

Mr. Sayed Ali Shah
Program Director HEADS

Miss. Ramsha Khan
HR Officer

Mr. Raza Ullah Jan
Executive Director

Mr. Muhammad Jidran
BOG Member

Miss. Ambareen Banori
BOG Member

Miss. Tahira Nasreen
BOG Member

Mr. Asif Ali
Director Operations HEADS

Policy Review & Update Record

A Board meeting was held on January 6, 2025, with the key agenda of reviewing and updating all organizational policies of HEADS. The Board advised the management to undertake a comprehensive policy review to ensure relevance, compliance, and alignment with organizational goals and evolving operational needs.

In line with this directive, all organizational policies were reviewed and amended on January 31, 2025, under the leadership of the Executive Director and with the involvement of the Finance & Audit Committee and relevant departments.

The review process included:

- A thorough evaluation of existing policies.
- Revisions based on internal assessments, audit findings, regulatory requirements, and best practices.
- Incorporation of feedback from staff and stakeholders.
- Updates to enhance clarity, accountability, and operational effectiveness.

Means of Verification:
Revised policy documents, review reports, and documented feedback and approval records.

Raza Ullah Jan
Executive Director